

Oracle® Audit Vault

Auditor's Guide

Release 10.2.3.2

E14460-07

September 2011

Oracle Audit Vault Auditor's Guide, Release 10.2.3.2

E14460-07

Copyright © 2007, 2011, Oracle and/or its affiliates. All rights reserved.

Primary Author: Patricia Huey

Contributing Author: Rodney Ward

Contributors: Tammy Bednar, Janet Blowney, Raghavendran Hanumantharau, Ravi Kumar, Srivatsan Kannan, K. Karun, Anurag Prasad, Vipul Shah, Prahlada Varadan Thirumalai, Lok Sheung, Srividya Tata

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. 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, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface	xiii
Audience	xiii
Documentation Accessibility	xiii
Related Documents	xiii
Conventions	xiv
What's New in Oracle Audit Vault for Auditors?	xv
Oracle Audit Vault Release 10.2.3.2 New Features	xv
Oracle Audit Vault Release 10.2.3.1 New Features	xxii
1 Introducing Oracle Audit Vault for Auditors	
1.1 How Do Auditors Use Oracle Audit Vault?	1-1
1.2 General Steps for Using Oracle Audit Vault.....	1-2
1.2.1 Step 1: Ensure That the Source Databases Are Collecting Audit Data	1-2
1.2.2 Step 2: Create Audit Policies for Oracle Database Data.....	1-2
1.2.3 Step 3: Optionally, Create and Monitor Alerts.....	1-3
1.2.4 Step 4: View and Customize the Oracle Audit Vault Reports	1-3
1.2.5 Step 5: Respond to Reports and Alerts	1-3
1.3 Database Requirements for Collecting Audit Data.....	1-4
1.3.1 Requirements for Oracle Database.....	1-4
1.3.1.1 Ensuring That Auditing Is Enabled in the Source Database.....	1-4
1.3.1.2 Using Recommended Audit Settings in the Source Database	1-5
1.3.2 Requirements for SQL Server, Sybase ASE, and IBM DB2 Databases.....	1-6
1.4 Starting the Oracle Audit Vault Console.....	1-6
1.5 Ensuring That the Oracle Audit Vault Collectors Can Collect Data	1-7
1.5.1 About Oracle Audit Vault Data Collection.....	1-8
1.5.2 Checking the Status of the Source Database Collection Agents	1-8
1.5.3 What Happens if the Source Database Collection Agents Were Not Active?	1-9
2 Creating Oracle Audit Vault Policies and Alerts	
2.1 About Oracle Audit Vault Policies and Alerts	2-1
2.2 General Steps for Creating Oracle Audit Vault Policies and Alerts.....	2-2
2.3 Retrieving Audit Policy Settings from the Source Oracle Database.....	2-2
2.3.1 Step 1: Retrieve the Audit Settings from the Source Oracle Database.....	2-2
2.3.2 Step 2: Activate (Update) the Fetched Audit Settings State	2-4

2.4	Creating Oracle Vault Audit Policies for SQL Statements.....	2-5
2.4.1	About SQL Statement Auditing.....	2-5
2.4.2	Defining a SQL Statement Audit Policy.....	2-6
2.5	Creating Oracle Audit Vault Policies for Schema Objects	2-8
2.5.1	About Schema Object Auditing.....	2-8
2.5.2	Defining a Schema Object Audit Policy	2-8
2.6	Creating Oracle Audit Vault Policies for Privileges	2-10
2.6.1	About Privilege Auditing.....	2-10
2.6.2	Defining a Privilege Audit Policy.....	2-11
2.7	Creating Oracle Audit Vault Policies for Fine-Grained Auditing	2-12
2.7.1	About Fine-Grained Auditing	2-12
2.7.1.1	Auditing Specific Columns and Rows	2-13
2.7.1.2	Using Event Handlers in Fine-Grained Auditing.....	2-13
2.7.2	Defining a Fine-Grained Auditing Policy	2-14
2.8	Creating Capture Rules for Redo Log File Auditing.....	2-17
2.8.1	About Capture Rules Redo Log File Auditing.....	2-17
2.8.2	Defining a Capture Rule for Redo Log File Auditing	2-17
2.9	Verifying Oracle Audit Vault Policy Settings.....	2-19
2.10	Provisioning Audit Vault Policies to the Source Oracle Database	2-19
2.10.1	Saving the Audit Policy Settings to a SQL Script for a Database Administrator	2-20
2.10.2	Manually Provisioning the Audit Policy Settings to the Source Database	2-20
2.11	Copying Oracle Audit Vault Policies to Other Oracle Databases.....	2-21
2.12	Creating and Configuring Alerts.....	2-21
2.12.1	About Alerts	2-21
2.12.2	Creating Templates to be Used for Alerts.....	2-22
2.12.2.1	About Notification Alert Templates	2-22
2.12.2.2	Creating an E-Mail Notification Profile.....	2-22
2.12.2.3	Creating an E-Mail Notification Template.....	2-23
2.12.2.4	Creating a Trouble Ticket Template	2-26
2.12.3	Creating Alert Status Values.....	2-29
2.12.4	Creating a Basic Alert.....	2-30
2.12.5	Creating an Advanced Alert	2-32
2.12.5.1	About Advanced Alerts.....	2-32
2.12.5.2	Creating an Advanced Alert That Uses a Condition.....	2-33
2.12.5.3	Creating an Advanced Alert Condition That Uses a Function.....	2-35
2.12.6	Monitoring Alerts	2-36
2.13	Responding to an Alert	2-38
2.14	Setting a Retention Period for Audit Data	2-39

3 Using Oracle Audit Vault Reports

3.1	What Are Oracle Audit Vault Reports?.....	3-1
3.2	Accessing the Oracle Audit Vault Audit Reports	3-1
3.3	Using the Default Reports	3-2
3.3.1	About the Default Reports.....	3-2
3.3.2	Using the Default Access Reports	3-3
3.3.2.1	About the Default Access Reports	3-3
3.3.2.2	Activity Overview Report	3-4

3.3.2.3	Data Access Report.....	3-4
3.3.2.4	Database Vault Report.....	3-5
3.3.2.5	Distributed Database Report	3-5
3.3.2.6	Procedure Executions Report	3-5
3.3.2.7	User Sessions Report.....	3-5
3.3.3	Using the Default Management Activity Reports.....	3-6
3.3.3.1	About the Default Management Activity Reports.....	3-6
3.3.3.2	Account Management Report.....	3-6
3.3.3.3	Audit Commands Report	3-6
3.3.3.4	Object Management Report	3-7
3.3.3.5	Procedure Management Report	3-7
3.3.3.6	Role and Privilege Management Report	3-7
3.3.3.7	System Management Report.....	3-8
3.3.4	Using the Default System Exception Reports.....	3-8
3.3.4.1	About the Default System Exception Reports.....	3-8
3.3.4.2	Exception Activity Report	3-8
3.3.4.3	Invalid Audit Record Report	3-8
3.3.4.4	Uncategorized Activity Report.....	3-9
3.3.5	Using the Default Entitlement Reports.....	3-9
3.3.5.1	About the Default Entitlement Reports.....	3-9
3.3.5.2	User Accounts Report and User Accounts by Source Report	3-10
3.3.5.3	User Privileges Report and User Privileges by Source Report	3-10
3.3.5.4	User Profiles Report and User Profiles by Source Report	3-10
3.3.5.5	Database Roles Report and Database Roles by Source Report	3-10
3.3.5.6	System Privileges Report and System Privileges by Source Report	3-11
3.3.5.7	Object Privileges Report and Object Privileges by Source Report	3-11
3.3.5.8	Privileged Users Report and Privileged Users by Source Report	3-11
3.4	Using the Compliance Reports	3-11
3.4.1	About the Compliance Reports	3-11
3.4.2	Credit Card Compliance Report: Related Data Access Compliance Report.....	3-12
3.4.3	Financial Compliance Reports	3-12
3.4.3.1	Financial Related Data Access Report	3-12
3.4.3.2	Financial Related Data Modifications Report.....	3-13
3.4.4	Health Care Compliance Report: EPHI Related Data Access Report	3-13
3.4.5	Common Credit Card, Financial, and Health Care Compliance Reports	3-13
3.4.5.1	Audit Setting Changes Report.....	3-13
3.4.5.2	Before/ After Values Report.....	3-13
3.4.5.3	Database Failed Logins Report.....	3-14
3.4.5.4	Database Login/Logoff Report	3-14
3.4.5.5	Database Logoff Report	3-14
3.4.5.6	Database Logon Report	3-14
3.4.5.7	Database Startup/Shutdown Report.....	3-14
3.4.5.8	Deleted Objects Report	3-14
3.4.5.9	Program Changes Report	3-14
3.4.5.10	Schema Changes Report	3-14
3.4.5.11	System Events Report	3-14
3.4.5.12	User Privilege Change Activity Report.....	3-15

3.5	Using the Critical and Warning Alert Reports	3-15
3.5.1	About the Critical and Warning Alert Reports	3-15
3.5.2	All Alerts Report	3-15
3.5.3	Critical Alerts Report	3-15
3.5.4	Warning Alerts Report.....	3-15
3.6	Scheduling and Creating PDF Reports	3-15
3.6.1	About Scheduling and Creating PDF Reports.....	3-15
3.6.2	Scheduling and Creating a PDF Report	3-16
3.7	Annotating and Attesting Reports	3-18
3.7.1	About Annotating and Attesting Reports.....	3-18
3.7.2	Annotating and Attesting a Report.....	3-18
3.8	Generating and Comparing Snapshots of Entitlement Audit Data.....	3-19
3.8.1	About Entitlement Report Snapshots and Labels	3-19
3.8.2	General Steps for Using Entitlement Reports.....	3-19
3.8.3	Retrieving Entitlement Audit Data to Create the Snapshot	3-20
3.8.4	Creating an Entitlement Snapshot Label.....	3-20
3.8.5	Assigning Snapshots to a Label	3-21
3.8.6	Viewing Entitlement Snapshot and Label Audit Data.....	3-22
3.8.6.1	About Viewing Entitlement Snapshot and Label Audit Data	3-22
3.8.6.2	Checking Entitlement Reports for Individual Snapshot or Label Audit Data .	3-22
3.8.6.3	Checking Entitlement Reports for Changes to Snapshot or Label Audit Data	3-23
3.9	Controlling the Display of Data in a Report	3-24
3.9.1	About Controlling the Display of Report Data	3-24
3.9.2	Hiding or Showing Columns in a Report	3-24
3.9.2.1	Hiding the Currently Selected Column.....	3-24
3.9.2.2	Hiding or Showing Any Column.....	3-25
3.9.3	Filtering Data in a Report	3-26
3.9.3.1	About Filtering Data in Reports	3-26
3.9.3.2	Filtering All Rows Based on Data from the Currently Selected Column.....	3-26
3.9.3.3	Filtering Column and Row Data	3-27
3.9.3.4	Filtering Row Data Using an Expression	3-28
3.9.4	Changing the Default Displayed Contents of a Compliance Report	3-29
3.9.5	Sorting Data in a Report	3-29
3.9.5.1	Sorting Row Data for the Currently Selected Column.....	3-30
3.9.5.2	Sorting Row Data for All Columns.....	3-30
3.9.6	Highlighting Rows in a Report.....	3-30
3.9.7	Charting Data in a Report.....	3-31
3.9.8	Adding a Control Break to a Column in a Report	3-32
3.9.9	Resetting the Report Display Values to Their Default Settings	3-33
3.10	Finding Information About Report Data.....	3-33
3.10.1	Finding Detailed Information About an Audit Record.....	3-33
3.10.2	Finding Information About the Purpose of a Column.....	3-33
3.11	Working with User-Defined Reports	3-34
3.11.1	About User-Defined Reports	3-34
3.11.2	Creating a Category for User-Defined Reports.....	3-34
3.11.2.1	Creating a Category Name.....	3-34
3.11.2.2	Alphabetizing the Category Name List.....	3-34

3.11.2.3	Editing a Category Name	3-34
3.11.3	Creating a User-Defined Report	3-35
3.11.4	Accessing a User-Defined Report.....	3-35
3.12	Downloading a Report to a CSV File	3-36

4 Oracle Audit Vault Data Warehouse Schema

4.1	About the Oracle Audit Vault Data Warehouse Schema	4-1
4.2	Oracle Audit Vault Audit Data Warehouse Architecture.....	4-1
4.3	Design of the Audit Data Warehouse Schema	4-2
4.4	How the Fact Table and Dimension Tables Work	4-3
4.5	Fact Table Constraints and Indexes.....	4-5
4.6	Relationships Between the Fact and Dimension Tables.....	4-6
4.6.1	AUDIT_EVENT_FACT Fact Table	4-7
4.6.2	CLIENT_HOST_DIM Dimension Table	4-13
4.6.3	CLIENT_TOOL_DIM Dimension Table.....	4-13
4.6.4	CONTEXT_DIM Dimension Table.....	4-13
4.6.5	EVENT_DIM Dimension Table	4-14
4.6.6	PRIVILEGES_DIM Dimension Table.....	4-14
4.6.7	SOURCE_DIM Dimension Table.....	4-15
4.6.8	TARGET_DIM Dimension Table.....	4-15
4.6.9	TIME_DIM Dimension Table.....	4-16
4.6.10	USER_DIM Dimension Table.....	4-18
4.7	Accessing Data Trace Values.....	4-18

A Oracle Database Audit Events

A.1	About the Oracle Database Audit Events.....	A-1
A.2	Account Management Events	A-2
A.3	Application Management Events	A-3
A.4	Audit Command Events	A-6
A.5	Data Access Events	A-7
A.6	Oracle Database Vault Events.....	A-9
A.7	Exception Events.....	A-10
A.8	Invalid Record Events	A-11
A.9	Object Management Events.....	A-13
A.10	Peer Association Events	A-16
A.11	Role and Privilege Management Events.....	A-17
A.12	Service and Application Utilization Events	A-18
A.13	System Management Events	A-20
A.14	Unknown or Uncategorized Events	A-22
A.15	User Session Events	A-23

B Microsoft SQL Server Audit Events

B.1	About the Microsoft SQL Server Audit Events	B-1
B.2	Account Management Events	B-2
B.3	Application Management Events	B-4
B.4	Audit Command Events	B-6

B.5	Data Access Events	B-7
B.6	Exception Events	B-9
B.7	Invalid Record Events	B-11
B.8	Object Management Events	B-13
B.9	Peer Association Events	B-16
B.10	Role and Privilege Management Events.....	B-17
B.11	Service and Application Utilization Events	B-20
B.12	System Management Events	B-21
B.13	Unknown or Uncategorized Events	B-24
B.14	User Session Events	B-26

C Sybase Adaptive Server Enterprise Audit Events

C.1	About the Sybase Adaptive Server Enterprise Audit Events.....	C-1
C.2	Account Management Events	C-2
C.3	Application Management Events	C-3
C.4	Audit Command Events	C-4
C.5	Data Access Events	C-6
C.6	Exception Events	C-7
C.7	Invalid Record Events	C-8
C.8	Object Management Events.....	C-9
C.9	Peer Association Events	C-11
C.10	Role and Privilege Management Events.....	C-12
C.11	Service and Application Utilization Events	C-13
C.12	System Management Events	C-15
C.13	Unknown or Uncategorized Events	C-17
C.14	User Session Events	C-18

D IBM DB2 Audit Events

D.1	About the IBM DB2 Audit Events	D-1
D.2	Account Management Events	D-2
D.3	Application Management Events	D-3
D.4	Audit Command Events	D-4
D.5	Data Access Events	D-5
D.6	Exception Events	D-6
D.7	Invalid Record Events	D-7
D.8	Object Management Events.....	D-8
D.9	Peer Association Events	D-10
D.10	Role and Privilege Management Events.....	D-10
D.11	Service and Application Utilization Events	D-12
D.12	System Management Events	D-13
D.13	Unknown or Uncategorized Events	D-15
D.14	User Session Events	D-16

Index

List of Figures

2-1	Dashboard Page	2-37
3-1	Default Reports Page	3-3
3-2	Activity Overview Report Page	3-4
3-3	Compliance Reports Page.....	3-12
3-4	Showing Individual Snapshot or Label Audit Data	3-23
3-5	Comparing Entitlement Report Snapshot or Label Audit Data.....	3-24
4-1	Architecture of the Oracle Audit Vault Audit Data Warehouse.....	4-2
4-2	Structure of the Oracle Audit Data Warehouse.....	4-3
4-3	Source Dimension Hierarchy	4-4
4-4	Tables in the Oracle Audit Vault Data Warehouse.....	4-6

List of Tables

1-1	Oracle Database Audit Trail Types and Corresponding Collectors.....	1-5
1-2	Database Collector Types Provided by Oracle Audit Vault.....	1-9
2-1	Fields Under Apply Audit Settings in the Audit Settings Page.....	2-3
2-2	Fields in the Statement Page.....	2-6
2-3	Fields in the Create Statement Audit Page.....	2-7
2-4	Fields in the Object Page.....	2-9
2-5	Fields in the Create Object Audit Page.....	2-9
2-6	Fields in the Privilege Page.....	2-11
2-7	Fields in the Create Privilege Audit Page.....	2-12
2-8	Fields in the Fine-Grained Audit Page.....	2-15
2-9	Fields in the Create Fine Grained Audit Page.....	2-15
2-10	Fields in the Capture Rule Page.....	2-18
2-11	Fields in the Create Capture Rule Page.....	2-19
2-12	Fields in the Add Notification Profile Page.....	2-23
2-13	Fields in the Add Notification Template Page.....	2-25
2-14	Notification Template Alert Tags.....	2-25
2-15	Notification Template Report Tags.....	2-26
2-16	Fields Used in the Add Trouble Ticket Template Page.....	2-27
4-1	Fact Table Constraints and Indexes.....	4-5
4-2	Local Bitmap Indexes Defined on the AUDIT_EVENT_FACT Table.....	4-5
4-3	AUDIT_EVENT_FACT Fact Table.....	4-7
4-4	CLIENT_HOST_DIM Dimension Table.....	4-13
4-5	CLIENT_TOOL_DIM Dimension Table.....	4-13
4-6	CONTEXT_DIM Dimension Table.....	4-13
4-7	EVENT_DIM Dimension Table.....	4-14
4-8	PRIVILEGES_DIM Dimension Table.....	4-14
4-9	SOURCE_DIM Dimension Table.....	4-15
4-10	TARGET_DIM Dimension Table.....	4-15
4-11	TIME_DIM Dimension Table.....	4-16
4-12	USER_DIM Dimension Table.....	4-18
A-1	Oracle Database Account Management Audit Events.....	A-2
A-2	Oracle Database Account Management Event Attributes.....	A-2
A-3	Oracle Database Application Management Audit Events.....	A-3
A-4	Oracle Database Application Management Event Attributes.....	A-5
A-5	Oracle Database Audit Command Audit Events.....	A-6
A-6	Oracle Database Audit Command Event Attributes.....	A-6
A-7	Oracle Database Data Access Audit Events.....	A-7
A-8	Oracle Database Data Access Event Attributes.....	A-7
A-9	Oracle Database Vault Audit Events.....	A-9
A-10	Oracle Database Vault Event Attributes.....	A-10
A-11	Oracle Database Exception Audit Events.....	A-10
A-12	Oracle Database Exception Event Attributes.....	A-10
A-13	Oracle Database Invalid Record Audit Events.....	A-12
A-14	Oracle Database Invalid Record Event Attributes.....	A-12
A-15	Oracle Database Object Management Audit Events.....	A-13
A-16	Oracle Database Object Management Event Attributes.....	A-14
A-17	Oracle Database Peer Association Audit Events.....	A-16
A-18	Oracle Database Peer Association Event Attributes.....	A-16
A-19	Oracle Database Role and Privilege Management Audit Events.....	A-17
A-20	Oracle Database Role and Privilege Management Event Attributes.....	A-17
A-21	Oracle Database Service and Application Utilization Audit Events.....	A-19
A-22	Oracle Database Service and Application Utilization Event Attributes.....	A-19
A-23	Oracle Database System Management Audit Events.....	A-20

A-24	Oracle Database System Management Event Attributes	A-21
A-25	Oracle Database Unknown or Uncategorized Audit Events.....	A-22
A-26	Oracle Database Unknown or Uncategorized Event Attributes.....	A-22
A-27	Oracle Database User Session Audit Events.....	A-23
A-28	Oracle Database User Session Event Attributes	A-24
B-1	SQL Server Account Management Events	B-2
B-2	SQL Server Account Management Event Attributes	B-2
B-3	SQL Server Application Management Audit Events.....	B-4
B-4	SQL Server Application Management Event Attributes.....	B-4
B-5	SQL Server Audit Command Audit Events.....	B-6
B-6	SQL Server Audit Command Events Logged in Windows Event Viewer	B-6
B-7	SQL Server Audit Command Event Attributes.....	B-6
B-8	SQL Server Data Access Audit Events.....	B-8
B-9	SQL Server Data Access Event Attributes.....	B-8
B-10	SQL Server Exception Audit Events	B-9
B-11	SQL Server Exception Events Logged in the Windows Event Viewer	B-9
B-12	SQL Server Exception Event Attributes.....	B-10
B-13	SQL Server Invalid Record Event Attributes.....	B-11
B-14	SQL Server Object Management Audit Events	B-13
B-15	SQL Server Object Management Event Attributes.....	B-14
B-16	SQL Server Peer Association Event Attributes.....	B-16
B-17	SQL Server Role and Privilege Management Audit Events	B-17
B-18	SQL Server Role and Privilege Management Event Attributes	B-18
B-19	SQL Server Service and Application Utilization Audit Events.....	B-20
B-20	SQL Server Service and Application Utilization Event Attributes.....	B-20
B-21	SQL Server System Management Audit Events	B-22
B-22	SQL Server System Management Event Attributes	B-23
B-23	SQL Server Unknown or Uncategorized Event Attributes.....	B-24
B-24	SQL Server Unknown or Uncategorized Event Attributes.....	B-25
B-25	SQL Server User Session Audit Events.....	B-26
B-26	SQL Server User Session Event Attributes.....	B-27
C-1	Sybase ASE Account Management Audit Events	C-2
C-2	Sybase ASE Account Management Event Attributes	C-2
C-3	Sybase ASE Application Management Audit Events.....	C-3
C-4	Sybase ASE Application Management Event Attributes	C-3
C-5	Sybase ASE Audit Command Audit Events.....	C-5
C-6	Sybase ASE Audit Command Event Attributes	C-5
C-7	Sybase ASE Data Access Audit Events.....	C-6
C-8	Sybase ASE Data Access Event Attributes	C-6
C-9	Sybase ASE Exception Audit Events.....	C-7
C-10	Sybase ASE Exception Event Attributes.....	C-7
C-11	Sybase ASE Invalid Record Event Attributes	C-8
C-12	Sybase ASE Object Management Audit Events.....	C-9
C-13	Sybase ASE Object Management Event Attributes.....	C-10
C-14	Sybase ASE Peer Association Event Attributes	C-11
C-15	Sybase ASE Role and Privilege Management Audit Events	C-12
C-16	Sybase ASE Role and Privilege Management Event Attributes.....	C-12
C-17	Sybase ASE Service and Application Utilization Audit Events.....	C-14
C-18	Sybase ASE Service and Application Utilization Event Attributes	C-14
C-19	Sybase ASE System Management Audit Events	C-15
C-20	Sybase ASE System Management Event Attributes	C-16
C-21	Sybase ASE Unknown or Uncategorized Audit Events.....	C-17
C-22	Sybase ASE Unknown or Uncategorized Event Attributes.....	C-17
C-23	Sybase ASE User Session Audit Events.....	C-18
C-24	Sybase ASE User Session Event Attributes	C-18

D-1	IBM DB2 Account Management Audit Events.....	D-2
D-2	IBM DB2 Account Management Event Attributes.....	D-2
D-3	IBM DB2 Application Management Audit Events.....	D-3
D-4	IBM DB2 Application Management Event Attributes.....	D-3
D-5	IBM DB2 Audit Command Audit Events.....	D-4
D-6	IBM DB2 Audit Command Event Attributes.....	D-5
D-7	IBM DB2 Data Access Audit Events.....	D-5
D-8	IBM DB2 Data Access Event Attributes.....	D-6
D-9	IBM DB2 Exception Event Attributes.....	D-6
D-10	IBM DB2 Invalid Record Event Attributes.....	D-7
D-11	IBM DB2 Object Management Audit Events	D-8
D-12	IBM DB2 Object Management Event Attributes	D-9
D-13	IBM DB2 Peer Association Event Attributes.....	D-10
D-14	IBM DB2 Role and Privilege Management Audit Events	D-10
D-15	IBM DB2 Role and Privilege Management Event Attributes	D-11
D-16	IBM DB2 Service and Application Utilization Audit Events.....	D-12
D-17	IBM DB2 Service and Application Utilization Event Attributes.....	D-12
D-18	IBM DB2 System Management Audit Events.....	D-13
D-19	IBM DB2 System Management Event Attributes	D-15
D-20	IBM DB2 Unknown or Uncategorized Audit Events	D-15
D-21	IBM DB2 Unknown or Uncategorized Event Attributes.....	D-16
D-22	IBM DB2 User Session Audit Events.....	D-16
D-23	IBM DB2 User Session Event Attributes.....	D-17

Preface

Oracle Audit Vault Auditor's Guide explains how Oracle Audit Vault auditors can use the Audit Vault Console to monitor database activity in Oracle, Microsoft SQL Server, Sybase Adaptive Server Enterprise, and IBM DB2 databases.

This preface contains:

- [Audience](#)
- [Documentation Accessibility](#)
- [Related Documents](#)
- [Conventions](#)

Audience

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

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Related Documents

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

- *Oracle Audit Vault Administrator's Guide*
- *Oracle Database Vault Administrator's Guide*
- *Oracle Database Security Guide*
- *Oracle Database Advanced Security Administrator's Guide*
- *Oracle Database Reference*

- *Oracle Streams Concepts and Administration*
- *Oracle Database Data Warehousing Guide*

Oracle Documentation Search Engine

To access the database documentation search engine directly, visit:

<http://tahiti.oracle.com/>

Oracle Technology Network (OTN)

You can download free release notes, installation documentation, updated versions of this guide, white papers, or other collateral from the Oracle Technology Network (OTN). Visit

<http://www.oracle.com/technetwork/index.html>

For security-specific information on OTN, visit

<http://www.oracle.com/technetwork/topics/security/whatsnew/index.html>

For the latest version of the Oracle documentation, including this guide, visit

<http://www.oracle.com/technetwork/documentation/index.html>

Oracle Audit Vault-Specific Sites

For OTN information specific to Oracle Audit Vault, visit

<http://www.oracle.com/technetwork/database/audit-vault/overview/index.html>

For the Oracle Audit Vault Discussion Forums, visit

<http://forums.oracle.com/forums/forum.jspa?forumID=391>

Oracle Store

Printed documentation is available for sale in the Oracle Store at:

<https://shop.oracle.com>

My Oracle Support (formerly Oracle*MetaLink*)

You can find information about security patches, certifications, and the support knowledge base by visiting My Oracle Support at:

<https://support.oracle.com>

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.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in Oracle Audit Vault for Auditors?

This section describes new features in Oracle Audit Vault that affect auditors, and provides pointers to additional information. These new features reflect changes since Release 10.2.3.1.

This section contains:

- [Oracle Audit Vault Release 10.2.3.2 New Features](#)
- [Oracle Audit Vault Release 10.2.3.1 New Features](#)

Oracle Audit Vault Release 10.2.3.2 New Features

This section contains:

- [Near Real Time Activity Monitoring](#)
- [User Entitlement Audit Data](#)
- [E-Mail Notifications for Alerts and Reports](#)
- [Trouble Ticket Notifications for Alerts](#)
- [Annotating and Attesting Alerts and Reports](#)
- [More Functionality for Advanced Alerts](#)
- [Scheduling Reports to be Sent to Other Users in PDF Format](#)
- [Additional and Changed Reports](#)
- [New and Changed Audit Events](#)
- [Oracle Audit Vault Console User Interface Enhancements](#)
- [New PL/SQL Package to Find Before and After Values in Redo Logs](#)

Near Real Time Activity Monitoring

Starting with this release, the Oracle Audit Vault data warehouse automatically refreshes, because Audit Vault can send thousands of audit records continuously to the repository. This feature enables the reports to reflect the up-to-the-latest collection point of the audit data content.

See [Chapter 4, "Oracle Audit Vault Data Warehouse Schema,"](#) for more information about the data warehouse.

User Entitlement Audit Data

This release introduces a new set of reports called **entitlement reports**. These reports capture privilege-related audit data from Oracle source databases, such as the types of privileges users have been granted, user account information, the system privileges that have been used in a source database, and so on.

To view the entitlement information, you retrieve it from the source databases, similar to retrieving audit policies from source databases. Each time the entitlement content is retrieved from the Oracle database, it creates a snapshot of the entitlement information, which records the state of the entitlement data at the time of retrieval. With this information, you can compare the snapshots of the entitlement content to see how it has changed over time. For example, you can find out how a user's set of privileges were changed, or what object privileges were modified, between snapshots.

See the following sections for more information:

- [Section 3.3.5](#) describes the entitlement reports
- [Section 3.8](#) describes how to create and work with snapshot audit data

E-Mail Notifications for Alerts and Reports

E-mail notifications have been integrated into the Oracle Audit Vault alerts and reports. This provides the ability to e-mail you and your security team when an alert has been triggered in Oracle Audit Vault. This way, you and your team can proactively review violations in the business processes or malicious activity. In addition, you can notify managers that a report is ready for their review of database activity performed by their database administrative team. The notification contains a link to the report from the Oracle Audit Vault console, or you can directly attach the report to the notification in PDF format.

See the following sections for more information:

- [Section 2.12.2.2](#) describes how to create an e-mail notification profile, which is an e-mail address list that you can associate with the e-mail.
- [Section 2.12.2.3](#) describes how to create an e-mail notification template, which provides boilerplate text for the e-mail notification.
- [Section 2.12](#) describes how to configure an alert to use the e-mail notification.
- [Section 3.6](#) describes how to send other users an e-mail notification for a report.

Trouble Ticket Notifications for Alerts

You now can configure Oracle Audit Vault alerts to automatically generate trouble ticket notifications. Currently, you can use this feature for BMC Remedy Service Management trouble ticketing systems.

See the following sections for more information:

- [Section 2.12.2.4](#) describes how to create a trouble ticket template, which contains boilerplate text to be used for the trouble ticket.
- [Section 2.12](#) describes how to configure an alert to use the trouble ticket notification.
- [Section 2.13](#) describes how to send a trouble ticket notification from an alert.

Annotating and Attesting Alerts and Reports

When you schedule a report, you can optionally assign other auditors to attest to the report. While reviewing the report in Oracle Audit Vault, you, the auditor, can

annotate the report with comments that will remain until the report is deleted. This enables you to create a record of all notes and attestations for the report in one place, with the most recent note and attestation listed first.

In addition to a record of all annotations and attestations, you can find additional detailed information about alerts and reports.

See the following sections for more information:

- [Section 3.6](#) describes how to assign other auditors to attest to a specific report.
- [Section 3.7](#) describes how to annotate and attest a report.

More Functionality for Advanced Alerts

When you create an alert, you can create either a basic alert or an advanced alert. The advanced alert enables you to create a condition that can trigger the alert. In this release, you can incorporate more SQL functionality in the advanced alert condition that provides the ability to compare a list of valid values to incoming audit data content. For example, you can compare if the database activity was performed on a trusted host. You also can create PL/SQL functions that help you to retrieve more data to be used as a basis for triggering the alert. And, as described elsewhere in this section, you can configure the alert to be automatically sent to other users or to trigger a trouble ticket.

See [Section 2.12.5](#) for more information.

Scheduling Reports to be Sent to Other Users in PDF Format

You now can schedule reports to be generated in PDF format and then send it to a list of recipient users and to other auditors to attest. You can design the report so that it only captures data within a specified window of time based on when the report is run, and set formatting standards such as header and footer information, and whether the report will appear in portrait or landscape orientation.

See [Section 3.6](#) for more information.

Additional and Changed Reports

This release of Oracle Audit Vault provides many additional compliance reports and entitlement reports, which are designed to help meet compliance regulations that were established by the Sarbanes-Oxley Act (SOX) and Health Insurance Portability and Accountability Act (HIPAA).

The following table describes how the reports have changed for this release.

Report Name	Category of Report	Change for This Release
Audit Setting Changes Report	All compliance reports	Previously called the Changes to Audit Report
Before/After Values Report	All compliance reports	Previously called the Data Change Report
Changes to Audit Report	Default compliance reports	Now called the Audit Setting Changes Report
Credit Card Related Data Access Report	Credit card compliance reports	New for this release
Data Change Report	Default compliance reports	Now called the Before/After Values Report

Report Name	Category of Report	Change for This Release
Database Failed Logins Report	All compliance reports	Previously called the Login Failures Report. Mostly the same as in earlier releases except that the report varies depending whether it is a credit card, financial, or health care compliance report.
Database Login/Logoff Report	All compliance reports	Previously called the Login/Logoff Report. Mostly the same as in earlier releases except that the report varies depending whether it is a credit card, financial, or health care compliance report.
Database Logoff Report	All compliance reports	Contains the user logoff information from the Login/Logoff Report. Mostly the same as in earlier releases except that the report varies depending whether it is a credit card, financial, or health care compliance report.
Database Logon Report	All compliance reports	Contains the user logon information from the Login/Logoff Report. Mostly the same as in earlier releases except that the report varies depending whether it is a credit card, financial, or health care compliance report.
Database Roles by Source Report	Default entitlement reports	New for this release
Database Roles Report	Default entitlement reports	New for this release
Database Startup/Shutdown Report	All compliance reports	New for this release
Data Change Report	Default compliance reports	Now called the Program Changes Report
DDL Report	Default compliance reports	Now called the Schema Changes Report
Deleted Objects Report	All compliance reports	Mostly the same as in earlier releases except that the report varies depending whether it is a credit card, financial, or health care compliance report
EPHI Related Data Access Report	Health care compliance report	New for this release
Financial Related Data Access Report	Financial compliance reports	New for this release
Financial Related Data Modifications Report	Financial compliance reports	New for this release
Login Failures Report	Default compliance reports	Now called the Database Failed Logins Report
Login/Logoff Report	Default compliance reports	Now called the Database Login/Logoff Report
Object Privileges by Source Report	Default entitlement reports	New for this release
Object Privileges Report	Default entitlement reports	New for this release
Privileged Users by Source Report	Default entitlement reports	New for this release

Report Name	Category of Report	Change for This Release
Privileged Users Report	Default entitlement reports	New for this release
Program Changes Report	All compliance reports	Previously called the Data Change Report. Mostly the same as in earlier releases except that the report varies depending whether it is a credit card, financial, or health care compliance report.
Schema Changes Report	All compliance reports	Previously called the DDL Report. Mostly the same as in earlier releases except that the report varies depending whether it is a credit card, financial, or health care compliance report.
System Events Report	All compliance reports	New for this release
System Privileges by Source Report	Default entitlement reports	New for this release
System Privileges Report	Default entitlement reports	New for this release
User Accounts by Source Report	Default entitlement reports	New for this release
User Accounts Report	Default entitlement reports	New for this release
User Privilege Change Activity Report	All compliance reports	New for this release
User Privileges by Source Report	Default entitlement reports	New for this release
User Privileges Report	Default entitlement reports	New for this release
User Profiles by Source Report	Default entitlement reports	New for this release
User Profiles Report	Default entitlement reports	New for this release

See the following sections for more information about the new reports:

- [Section 3.4](#) describes the new compliance reports.
- [Section 3.3.5](#) describes the new entitlement reports.

New and Changed Audit Events

This section contains:

- [New and Changed Oracle Database Audit Events](#)
- [New Microsoft SQL Server Audit Events](#)

New and Changed Oracle Database Audit Events

This section contains:

- [New Audit Events for Oracle Database 11g Release 2 \(11.2\)](#)
- [Oracle Label Security Audit Events for All Supported Oracle Database Releases](#)
- [Changed Oracle Database Audit Events](#)

New Audit Events for Oracle Database 11g Release 2 (11.2) Starting with this release, Oracle Audit Vault supports the following new audit events that were added to Oracle Database 11g Release 2 (11.2).

Event Name Description	Source Event	Oracle Audit Vault Category
ALTER ASSEMBLY	217	Application Management
ALTER FLASHBACK ARCHIVE	219	System Management
ALTER EDITION	213	Object Management
ALTER MINING MODEL	130	Object Management
ALTER PUBLIC SYNONYM	134	Object Management
ALTER SYNONYM	192	Object Management
CREATE ASSEMBLY	216	Application Management
CREATE FLASHBACK ARCHIVE	218	System Management
CREATE EDITION	212	Object Management
CREATE MINING MODEL	133	Object Management
DROP ASSEMBLY	215	Application Management
DROP EDITION	214	Object Management
DROP FLASHBACK ARCHIVE	220	System Management
SELECT MINING MODEL	131	Data Access
SUPER USER TRANSACTION CONTROL	20000	System Management

See [Appendix A, "Oracle Database Audit Events,"](#) for more information.

Oracle Label Security Audit Events for All Supported Oracle Database Releases You can use the following Oracle Label Security-specific audit events for all supported Oracle Database Releases.

Event Name Description	Source Event	Oracle Audit Vault Category
APPLY TABLE OR SCHEMA POLICY	500	Object Management
OBJECT EXISTS ERRORS	505	Role and Privilege Management
PRIVILEGED ACTION	506	Role and Privilege Management
REMOVE TABLE OR SCHEMA POLICY	501	Object Management
SET USER OR PROGRAM UNIT LABEL	502	Role and Privilege Management

See [Appendix A, "Oracle Database Audit Events,"](#) for more information.

Changed Oracle Database Audit Events The following Oracle Database source events have changed:

Event Name Description	Previous Source Event	New Source Event
SHUTDOWN	216	20005
STARTUP	215	20004
SUPER USER DDL	213	20002
SUPER USER DML	214	20003
SUPER USER LOGON	212	20001
SUPER USER UNKNOWN	217	20006

See [Appendix A, "Oracle Database Audit Events,"](#) for more information.

New Microsoft SQL Server Audit Events

For Microsoft SQL Server 2008, the following new events have been added to the User Session Events category.

Event Name Description	Source Event	Audit Vault Event
Audit Database Mirroring Login Event	DATABASE MIRRORING LOGIN:LOGIN SUCCESS	LOGON
	DATABASE MIRRORING LOGIN:LOGIN PROTOCOL ERROR	
	DATABASE MIRRORING LOGIN:MESSAGE FORMAT ERROR	
	DATABASE MIRRORING LOGIN:NEGOTIATE FAILURE	
	DATABASE MIRRORING LOGIN:AUTHENTICATION FAILURE	
	DATABASE MIRRORING LOGIN:AUTHORIZATION FAILURE	

See [Section B.14](#) for more information.

Oracle Audit Vault Console User Interface Enhancements

The Audit Vault Console has the following new enhancements:

- **Dashboard.** The Dashboard, accessible from the **Home** tab, has been expanded to include the following new information:
 - Recently raised alerts, including all warning and critical alerts
 - Top five objects accessed
 - Failed logins
 - Report accession actions for the auditor who has logged into the Audit Vault Auditor console

The following components from earlier releases of Oracle Audit Vault are still available:

- View data time ranges
 - Alert severity summary
 - Summary of alert activity
 - Top five audit source by number of alerts
 - Alerts by audit event category
- **Statement, Object, Privilege, FGA, and Capture Rules Audit Settings pages.** The audit settings pages for statements, object privileges, fine-grained auditing, and capture rules now have a **Mark All as Not Needed** button. If you have set one or more policies as being needed (for example, by clicking the **Mark All as Needed** button) and realize that this was not a good idea, you can reverse the action by clicking the **Mark All as Not Needed** button.
 - **Audit Settings page.** This page now has the following new functionality:
 - **User Entitlement option.** This option enables you to retrieve user entitlement (privileges) information from the source databases. See "[User Entitlement Audit Data](#)" on page xvi for more information.

- **Check boxes for individual source databases.** You now can select one or more source databases and then perform a bulk retrieval of the audit policies and user entitlement information from the selected source databases. To select all the source databases, select the **Select All** link; to remove them from selection, select **Select None**.
- **Settings tab.** This tab provides access to pages that enable you to configure the following new features: notification profiles, notification templates, trouble ticket templates, and alert statuses. It also provides access to the Collector Status page.

New PL/SQL Package to Find Before and After Values in Redo Logs

This release introduces the `AVSYS.AV$DW_BEFORE_AFTER` PL/SQL package, which you can use to include before and after values collected by the REDO collector in your queries.

See [Section 4.7](#) for more information.

Oracle Audit Vault Release 10.2.3.1 New Features

This section contains:

- [Audit Events for Sybase ASE and IBM DB2 Databases](#)

Audit Events for Sybase ASE and IBM DB2 Databases

Starting with this release, you can generate reports that have audit events for Sybase Adaptive Server (ASE) and IBM DB2 databases. The supported releases for these two database products are as follows:

- **Sybase ASE:** ASE 12.5.4 and ASE 15.0.2 on platforms based on Linux and UNIX, and on Microsoft Windows platforms
- **IBM DB2:** IBM DB2 Version 8.2 and Version 9.5 on platforms based on Linux and UNIX, and on Microsoft Windows platforms. If you are using Version 8.2, ensure that you have installed Fixpack 16.

See the following sections for more information:

- [Appendix C, "Sybase Adaptive Server Enterprise Audit Events"](#)
- [Appendix D, "IBM DB2 Audit Events"](#)

Introducing Oracle Audit Vault for Auditors

This chapter contains:

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

1.1 How Do Auditors Use Oracle Audit Vault?

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

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

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

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

The audit policies feature lets you manage audit policies for Oracle Database source databases. Because Oracle Audit Vault centralizes audit settings for Oracle Database,

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

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

1.2 General Steps for Using Oracle Audit Vault

To use Oracle Audit Vault, follow these general steps:

- [Step 1: Ensure That the Source Databases Are Collecting Audit Data](#)
- [Step 2: Create Audit Policies for Oracle Database Data](#)
- [Step 3: Optionally, Create and Monitor Alerts](#)
- [Step 4: View and Customize the Oracle Audit Vault Reports](#)
- [Step 5: Respond to Reports and Alerts](#)

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

Check that auditing is enabled in the databases from which you want to collect audit data and that the Oracle Audit Vault collectors are working. For source databases, there are recommended audit settings that your database administrator should consider having in place. Your database administrator also should ensure that these databases are properly configured to send audit data to the Audit Vault Server.

See [Section 1.3](#) and [Section 1.5](#) for more information.

1.2.2 Step 2: Create Audit Policies for Oracle Database Data

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

You can create policies for the following kinds of data:

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

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

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

1.2.3 Step 3: Optionally, Create and Monitor Alerts

You can create either warnings or critical alerts that are triggered when certain events occur in an Oracle Database, SQL Server, Sybase ASE, or IBM DB2 database. You can configure the e-mail notifications or trouble tickets in response to the alert. Oracle Audit Vault alerts enable you to detect threats, which helps keep systems in compliance with internal and external policies. After you create the alerts, you can monitor them in the Audit Vault Console.

[Section 2.12](#) explains how you can configure e-mail and trouble ticket notifications, and create and monitor alerts.

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

Oracle Audit Vault automatically populates its reports with the audit data from your source databases. You can view this data by selecting from the reports provided in the Audit Vault Console Default Reports, Compliance Reports, and User-Defined Reports pages. The reports are organized by commonly used categories, including categories for compliance regulations.

You can perform the following actions with the reports:

- Create user-defined reports to filter specific data.
- Send the report to other users as a PDF file.
- Schedule the report to be generated at specific times and then sent to users as a PDF file. You can create an e-mail distribution list, called a profile, to be used specifically for different types of reporting and alert activities.

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

[Chapter 3, "Using Oracle Audit Vault Reports"](#) explains how to view and customize Oracle Audit Vault reports.

1.2.5 Step 5: Respond to Reports and Alerts

At this stage, the Oracle Audit Vault reports and alerts are generating as Audit Vault monitors your source databases.

When you review an Audit Vault report, you can annotate and attest the report, which is described in [Section 3.7](#).

When you are notified of an alert, you can take the following actions:

- Notify other users of the alert so that they can take the appropriate actions.
- Log a trouble ticket if one is necessary. In this release, you can log trouble tickets to the BMS Remedy Service Management trouble ticketing system. You can design trouble ticket templates to be used for different types of trouble ticket scenarios.
- View notes that other users may have created for the alert report.
- Set a status for the alert, such as `NEW` or `CLOSED`.

[Section 2.13](#) explains how to respond to an alert.

1.3 Database Requirements for Collecting Audit Data

This section contains:

- [Requirements for Oracle Database](#)
- [Requirements for SQL Server, Sybase ASE, and IBM DB2 Databases](#)

1.3.1 Requirements for Oracle Database

This section contains:

- [Ensuring That Auditing Is Enabled in the Source Database](#)
- [Using Recommended Audit Settings in the Source Database](#)

1.3.1.1 Ensuring That Auditing Is Enabled in the Source Database

Before Oracle Audit Vault can collect audit data from the source databases, auditing must be enabled in those databases. A database administrator can check the type of auditing your database uses by logging in to SQL*Plus and running the appropriate command.

For example, to check if standard auditing is enabled:

```
SQL> SHOW PARAMETER AUDIT_TRAIL
```

NAME	TYPE	VALUE
-----	-----	-----
audit_trail	string	DB

This output shows that standard auditing is enabled and audit records are being written to the database audit trail.

For fine-grained auditing, you can query the `AUDIT_TRAIL` column of the `DBA_AUDIT_POLICIES` data dictionary view to find the audit trail types that are set for the fine-grained audit policies on the database. For more information, see *Oracle Database Security Guide*.

Table 1–1 describes the audit trail types and their corresponding Audit Vault collectors.

Table 1–1 Oracle Database Audit Trail Types and Corresponding Collectors

Audit Trail Type	How Enabled	Corresponding Collector
Database audit trail	<p>For standard audit records: The <code>AUDIT_TRAIL</code> initialization parameter is set to <code>DB</code> or <code>DB, EXTENDED</code>.</p> <p>For fine-grained audit records: The <code>audit_trail</code> parameter of the <code>DBMS_FGA.ADD_POLICY</code> procedure is set to <code>DBMS_FGA.DB</code> or <code>DBMS_FGA.DB + DBMS_FGA.EXTENDED</code>.</p>	DBAUD
Operating system audit trail	<p>For standard audit records: The <code>AUDIT_TRAIL</code> initialization parameter is set to <code>OS</code>, <code>XML</code>, or <code>XML, EXTENDED</code>.</p> <p>For syslog audit trails, <code>AUDIT_TRAIL</code> is set to <code>OS</code> and the <code>AUDIT_SYS_OPERATIONS</code> parameter is set to <code>TRUE</code>. In addition, the <code>AUDIT_SYSLOG_LEVEL</code> parameter must be set.</p> <p>For fine-grained audit records: The <code>audit_trail</code> parameter of the <code>DBMS_FGA.ADD_POLICY</code> procedure is set to <code>DBMS_FGA.XML</code> or <code>DBMS_FGA.XML + DBMS_FGA.EXTENDED</code>.</p>	OSAUD
Redo log files	<p>The table that you want to audit must be eligible. See "Creating Capture Rules for Redo Log File Auditing" on page 2-17 for more information.</p>	REDO

1.3.1.2 Using Recommended Audit Settings in the Source Database

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

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

- AUDIT CREATE SESSION BY ACCESS;
- AUDIT CREATE USER BY ACCESS;
- AUDIT DROP PROFILE BY ACCESS;
- AUDIT DROP USER BY ACCESS;
- AUDIT EXEMPT ACCESS POLICY BY ACCESS;
- AUDIT GRANT ANY OBJECT PRIVILEGE BY ACCESS;
- AUDIT GRANT ANY PRIVILEGE BY ACCESS;
- AUDIT GRANT ANY ROLE BY ACCESS;
- AUDIT ROLE BY ACCESS;

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

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

1.4 Starting the Oracle Audit Vault Console

To start the Audit Vault Console:

1. From a browser, enter the following URL:

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

In this specification:

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

For example:

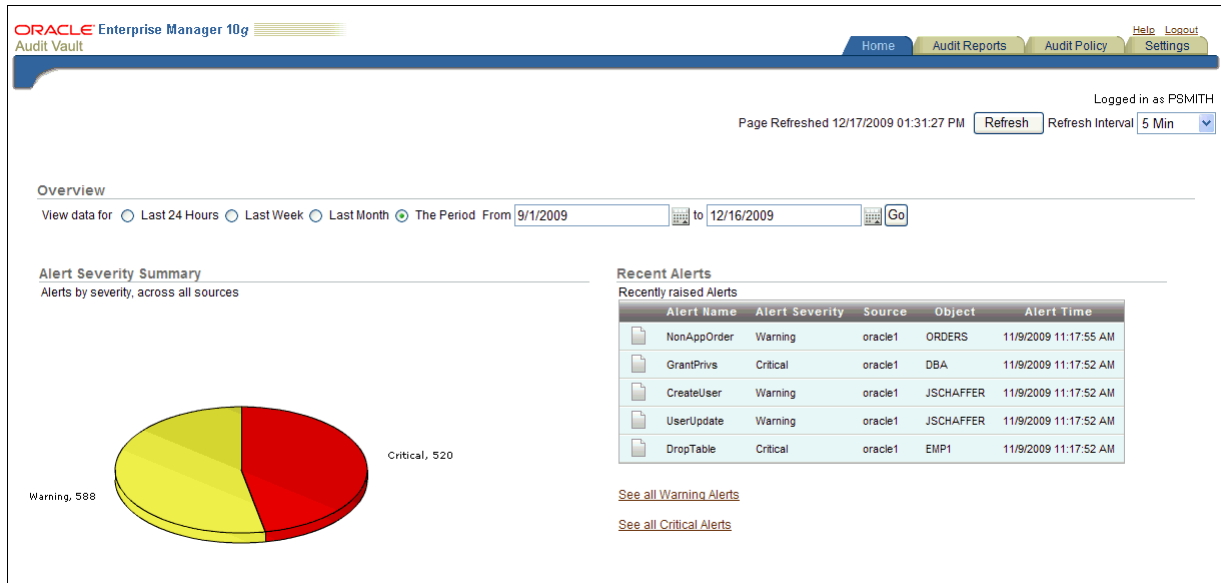
```
http://192.0.2.1:5700/av
```

If you are unsure of the URL, from the terminal window that you use for the Audit Vault Server, enter the following command, which displays the URL that starts the Audit Vault Console:

```
$ avctl show_av_status
```

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

The Dashboard page appears and displays information about configured alerts and audit trail activity.



From the Dashboard page, you can do the following:

- View audit data from a range of dates.** To view the audit data, which includes data such as the top five objects accessed and failed logins, specify the range you want, and then click the **Go** button. To automatically refresh the data every 60 seconds, click the **Refresh every 60 seconds** check box, or manually refresh it by clicking the **Refresh** button.
- Check alerts.** The Dashboard page displays recently raised alerts, as well as all warning and critical alerts.
- Check attestation actions.** The Dashboard page displays a list of reports that you may need to attest.
- Create Oracle Database audit policies and alerts.** [Chapter 2, "Creating Oracle Audit Vault Policies and Alerts"](#) explains how to create policies and alerts for an Oracle database.
- Access audit reports.** You can view audit information that has been collected in the Oracle Audit Vault reports. Optionally, you can control the display of data and create user-defined reports. See [Chapter 3, "Using Oracle Audit Vault Reports"](#) for more information.
- Ensure that the Oracle Audit Vault collection agents are working.** [Section 1.5](#) explains how to ensure that these agents are collecting audit data.

1.5 Ensuring That the Oracle Audit Vault Collectors Can Collect Data

This section contains:

- [About Oracle Audit Vault Data Collection](#)
- [Checking the Status of the Source Database Collection Agents](#)
- [What Happens if the Source Database Collection Agents Were Not Active?](#)

1.5.1 About Oracle Audit Vault Data Collection

The Oracle Audit Vault collection agents are responsible for the connection between the source database and the Audit Vault Server while collectors collect the audit data. In the Audit Vault Console, you can check the status of the collection agents and collectors. If you cannot access Oracle Database audit policies, or if the Oracle Audit Vault default reports do not show any information, then the collection agents may not be working, or the source database has been shut down. See also *Oracle Audit Vault Administrator's Guide* for additional troubleshooting tips for the reports.

1.5.2 Checking the Status of the Source Database Collection Agents

To check the status of the source database collection agents:

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

[Section 1.4](#) explains how to log in to the Audit Vault Console.

2. Click the **Settings** tab.
3. Click the **Collection Status** secondary tab.

The Collection Status page shows the following information for collectors:

- **Source name.** The name of the audit source database where the audit data is being collected
- **Collector Name.** Name of the collector
- **Agent Name.** The name of the agent with which this collector is associated
- **Bytes Per Sec.** Number of bytes per second it takes to retrieve the audit data
- **Records Per Sec.** Number of audit records that are being retrieved per second
- **Is Alive.** Whether the collector is running or not. When the collector is up, a green up arrow indicator is displayed. When the collector is down, a red down arrow indicator is displayed. When there is a problem, an error is displayed. If the collector is not working, then contact your Oracle Audit Vault administrator.

Table 1–2 summarizes the database collector types.

Table 1–2 Database Collector Types Provided by Oracle Audit Vault

Database	Collectors	Description
Oracle	DBAUD	Collector that performs the following: <ul style="list-style-type: none"> Extracts audit records from the Oracle Database audit trail. For the standard audit trail, it extracts records from the <code>SYS.AUD\$</code> system table. For fine-grained auditing, it extracts audit events from the <code>SYS.FGA_LOG\$</code> system table. Extracts audit records from the Oracle Database Vault audit trail <code>DVSYSTEM.AUDIT_TRAIL\$</code> table
Oracle	OSAUD	Collector that performs the following: <ul style="list-style-type: none"> For Linux and UNIX platforms: Extracts audit records from the operating system files (audit logs) and XML (.xml) files For Linux and UNIX platforms: SYSLOG Collector to extract audit records from the system audit trail where database audit trail records are written to a syslog file For Microsoft Windows: EVTLOG Collector to extract audit records from the system audit trail where database audit trail records are written to the Event Log
Oracle	REDO	Collector using Oracle Streams technology to retrieve logical change records from the redo logs.
SQL Server	MSSQLDB	Collector (for Windows platforms) to extract audit records from Microsoft SQL Server databases from the Windows Event logs, Server-side trace files, and C2 auditing logs.
Sybase ASE	SYBDB	Collector to extract audit records from the Sybase databases audit trail logged in audit tables in the SYBSECURITY database.
IBM DB2	DB2DB	Collector to extract records from the ASCII text file in which IBM DB2 generates audit data.

1.5.3 What Happens if the Source Database Collection Agents Were Not Active?

If the collection agents were not active, then no audit data is lost, as long as the source database continues to collect the audit data. When you restart the collection agent, it captures the audit data that the source database had collected during the time the collection agent was inactive.

Creating Oracle Audit Vault Policies and Alerts

This chapter contains:

- About Oracle Audit Vault Policies and Alerts
- General Steps for Creating Oracle Audit Vault Policies and Alerts
- Retrieving Audit Policy Settings from the Source Oracle Database
- Creating Oracle Vault Audit Policies for SQL Statements
- Creating Oracle Audit Vault Policies for Schema Objects
- Creating Oracle Audit Vault Policies for Privileges
- Creating Oracle Audit Vault Policies for Fine-Grained Auditing
- Creating Capture Rules for Redo Log File Auditing
- Verifying Oracle Audit Vault Policy Settings
- Provisioning Audit Vault Policies to the Source Oracle Database
- Copying Oracle Audit Vault Policies to Other Oracle Databases
- Creating and Configuring Alerts
- Responding to an Alert
- Setting a Retention Period for Audit Data

2.1 About Oracle Audit Vault Policies and Alerts

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

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

For all database types, you can create alerts. See [Section 2.12](#) for more information.

2.2 General Steps for Creating Oracle Audit Vault Policies and Alerts

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

1. Retrieve the current policy settings from the source Oracle database.
See [Section 2.3](#) for more information.
2. Create audit policies.
See the following sections:
 - [Section 2.4](#) to create SQL statement policies
 - [Section 2.5](#) to create schema object policies
 - [Section 2.6](#) to create privilege policies
 - [Section 2.7](#) to create fine-grained auditing policies
 - [Section 2.8](#) to create capture rules for redo log file auditing
 - [Section 2.9](#) to verify the Oracle Audit Vault policies
3. Save the Oracle Audit Vault policy settings to a .sql file or manually provision them to the source database.
See the following sections:
 - [Section 2.10](#) to export the policies to the source Oracle database
 - [Section 2.11](#) to copy the policy settings to other Oracle databases
4. Optionally, create alerts.
See [Section 2.12](#) for more information.
5. Optionally, set a retention period for the audit data from all source databases.
See [Section 2.14](#) for more information.

2.3 Retrieving Audit Policy Settings from the Source Oracle Database

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

Follow these steps:

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

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

To retrieve audit settings from the source Oracle Database:

1. Log in to the Audit Vault Console as a user who has been granted the AV_AUDITOR role.
[Section 1.4](#) explains how to start the Audit Vault Console. The Dashboard page appears.
2. In the Audit Vault Console, select the **Audit Policy** tab.
By default, the Audit Settings page appears.

- From the Audit Source listing, select the check boxes for the source databases you want.

The screenshot shows the Oracle Enterprise Manager 10g Audit Vault interface. At the top, there are navigation tabs for Home, Audit Reports, Audit Policy, and Help/Logout. The main content area is titled 'Audit Settings' and includes a search bar for 'Audit Source' with a 'Go' button. Below the search bar, there are radio buttons for 'Audit Settings' (selected) and 'User Entitlement', along with 'Retrieve' and 'Show Status' buttons. A table lists audit sources with columns for 'Select', 'Audit Source', 'In Use', 'Needed', 'Problem', 'Audit Trail', 'Audit Sys', 'Audit Settings Retrieved', 'Audit Settings Provisioned', and 'User Entitlement Retrieved'. The table contains one row for 'oracle1' with values: In Use: 94, Needed: 80, Problem: 14, Audit Trail: DB EXTENDED, Audit Sys: TRUE, Audit Settings Retrieved: Oct 6, 2009 8:26:27 AM GMT-07:00, and User Entitlement Retrieved: Oct 16, 2009 8:31:06 AM GMT-07:00. Below the table, the 'Audit Data Retention' section states that by default, Audit Vault retains collected audit data for 10 years. A field labeled 'Retain audit data for' is set to 10 years, with a 'Go' button.

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

- Click the **Audit Settings** option.
- Click the **Retrieve** button.

Oracle Audit Vault displays a message letting you know that the audit policy data is being retrieved. To check the status of the retrieval, click the **Show Status** button.

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

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

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

Field	Description
Select	Select the audit source to retrieve
Audit Source	Displays the name of the audit source database
In Use	Number of active settings in the source database
Needed	Number of required audit settings you (the auditor) have specified
Problem	Number of audit settings that require attention by the auditor

Table 2–1 (Cont.) Fields Under Apply Audit Settings in the Audit Settings Page

Field	Description
Audit Trail	The location to which database audit records are directed, based on the AUDIT_TRAIL initialization parameter. See <i>Oracle Database Reference</i> for the AUDIT_TRAIL parameter values. If the setting is NONE, then ask the database administrator to enable auditing. See Section 1.3.1.1 for more information.
Audit Sys	Indicates that the SYS user is being audited
Audit Setting Retrieved	The time that the audit information for the selected audit source was last retrieved
Audit Setting Provisioned	The time that the audit settings were provisioned to the source database
User Entitlement Retrieved	The time that the user entitlement information was retrieved. See Section 3.8 for more information.

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

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

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

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

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

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"/>	Statement	35	35	0
<input checked="" type="checkbox"/>	Object	4	4	0
<input checked="" type="checkbox"/>	Privilege	30	30	0
<input checked="" type="checkbox"/>	FGA	4	4	0
<input checked="" type="checkbox"/>	Capture Rule	21	21	0

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

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

Statement	User	Proxy User	Execution Condition	Audit Granularity	In Use	Needed
ROLE	FRIPON		Both	BY ACCESS	↑	✓
SYSTEM AUDIT	FRIPON		Both	BY ACCESS	↑	✓
EXECUTE PROCEDURE	FRIPON		Both	BY SESSION	↑	✓
INDEX	FRIPON		Both	BY ACCESS	↑	✓
SYSTEM GRANT	FRIPON		Both	BY ACCESS	↑	✓
DATABASE LINK	FRIPON		Both	BY ACCESS	↑	✓
GRANT TABLE	FRIPON		Both	BY ACCESS	↑	✓
DIMENSION	FRIPON		Both	BY ACCESS	↑	✓

3. Select each X in the **Needed** column to update the audit settings for SQL statements. Alternatively, click the **Mark All as Needed** button select all the audit settings. To deselect all of the selected settings, click **Mark All as Not Needed**.

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

4. After completing the **Needed** column updates, click the **Save All Audit Settings** button.

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

2.4 Creating Oracle Vault Audit Policies for SQL Statements

This section contains:

- [About SQL Statement Auditing](#)
- [Defining a SQL Statement Audit Policy](#)

2.4.1 About SQL Statement Auditing

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

- **Data definition statements (DDL).** For example, `AUDIT TABLE` audits all `CREATE TABLE` and `DROP TABLE` statements. `AUDIT TABLE` tracks several DDL statements

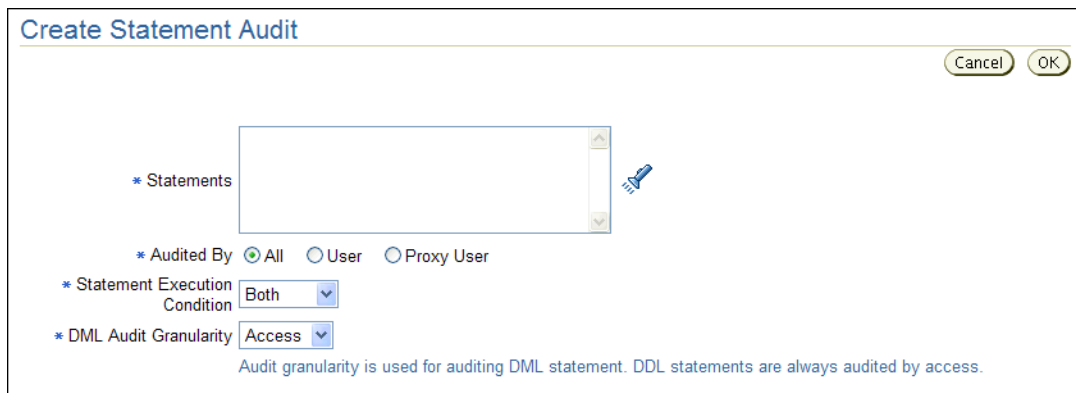
regardless of the table on which they are issued. You can also set statement auditing to audit selected users or every user in the database.

- **Data manipulation statements (DML).** For example, `AUDIT SELECT TABLE` audits all `SELECT ... FROM TABLE` or `SELECT ... FROM VIEW` statements, regardless of the table or view.

2.4.2 Defining a SQL Statement Audit Policy

To define a SQL statement audit policy:

1. If necessary, retrieve and activate the current statement audit policies.
See [Section 2.3](#) for more information.
2. In the Audit Settings page, select the **Statement** tab to display the Statement page.
[Table 2–2](#) on page 2-6 describes the fields used in the Statement page.
3. Click the **Create** button and in the Create Statement Audit page, define the audit policy.



[Table 2–3](#) on page 2-7 describes the Create Statement Audit fields.

4. Click **OK**.
The statement audit policy is created. To ensure that the statement audit policy is semantically correct, see [Section 2.9](#).
5. In the Dashboard page, select **Save All Audit Settings**.
To display the Dashboard page, click the **Audit Settings** link, and then in the Audit Settings page, select the name of the source database.

[Table 2–2](#) lists the fields used in the Statement page.

Table 2–2 Fields in the Statement Page

Field	Description
(Leftmost column)	An exclamation mark icon indicates one of the following conditions: <ul style="list-style-type: none"> ■ The statement is needed but is not in use. ■ The statement is in use but is not needed.
Statement	The statement that is audited
User	The user to which this setting applies, if any

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

Field	Description
Proxy User	The proxy user for the database, if any
Execution Condition	The execution condition audited: <code>WHENEVER SUCCESSFUL</code> , <code>WHENEVER NOT SUCCESSFUL</code> , or <code>BOTH</code>
Audit granularity	The granularity of auditing: <code>BY ACCESS</code> or <code>BY SESSION</code>
In Use	The arrow points upward if the setting is active in the source database and downward if it has not been provisioned or is not active.
Needed	<p>A check mark indicates that the policy is needed. An X indicates that the policy is not needed. If a policy that is not in use is set to needed, the In Use arrow points up after provisioning. If a policy that is in use is set to not needed, the audit policy is no longer displayed after provisioning.</p> <p>To select all policies as needed, click the Mark All as Needed button. To reverse this action, click Mark All as Not Needed.</p>
(Rightmost column)	Click the trash can icon to remove the policy. You can use the trash can icon to remove the policy only if you had just created it and decided it was not required in the source database, or if it is not active in the source database.

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

Table 2–3 Fields in the Create Statement Audit Page

Field	Description
Statements	<p>Select the SQL statements to audit. To display the list of SQL statements for selection, click the flashlight icon.</p> <p>Examples are:</p> <ul style="list-style-type: none"> ■ ALTER TABLE ■ DATABASE LINK ■ DROP DIRECTORY
Audited By	<p>Choose the category of users to audit:</p> <ul style="list-style-type: none"> ■ All: Audits all users, including proxy users. ■ User: Audits the user to which this setting applies. When you select this option, the Users field appears, in which you must specify at least one user. To display a list of users and their audit sources for selection, click the flashlight icon. ■ Proxy User: Audits the proxy user for the database. When you select this option, the Proxy User field appears, in which you must specify at least one user. To display a list of proxy users and their audit sources for selection, click the flashlight icon.
Statement Execution Condition	<p>Choose the execution condition:</p> <ul style="list-style-type: none"> ■ Both: Audits both successful and failed statements ■ Success: Audits the statement if it is successful ■ Failure: Audits the statement if it fails

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

Field	Description
DML Audit Granularity	Choose the level of granularity: <ul style="list-style-type: none"> ▪ Access: Creates an audit record each time the operation occurs ▪ Session: Creates an audit record the first time an operation occurs in the current session

2.5 Creating Oracle Audit Vault Policies for Schema Objects

This section contains:

- [About Schema Object Auditing](#)
- [Defining a Schema Object Audit Policy](#)

2.5.1 About Schema Object Auditing

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

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

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

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

2.5.2 Defining a Schema Object Audit Policy

To define a schema object audit policy:

1. If necessary, retrieve and activate the current object audit policies.
See [Section 2.3](#) for more information.
2. In the Audit Settings page, select the **Object** tab to display the Object page.
[Table 2–4](#) on page 2-9 describes the fields used in the Object page.
3. Click the **Create** button and in the Create Object Audit page, define the audit policy.
[Table 2–5](#) on page 2-9 describes the Create Object Audit fields.
4. Click **OK**.

The object audit policy is created. To ensure that the object audit policy is semantically correct, see [Section 2.9](#).

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

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

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

Table 2–4 Fields in the Object Page

Field	Description
(Leftmost column)	An exclamation mark icon indicates one of the following conditions: <ul style="list-style-type: none"> ■ The statement is needed but is not in use. ■ The statement is in use but is not needed.
Statement	The statement that is audited
Schema	The database schema to which this setting applies
Object	The object (such as a database table) to which this setting applies
Execution Condition	The execution condition audited: <code>WHENEVER SUCCESSFUL</code> , <code>WHENEVER NOT SUCCESSFUL</code> , or <code>BOTH</code>
Audit granularity	The granularity of auditing: <code>BY ACCESS</code> or <code>BY SESSION</code>
In Use	The arrow points upward if the setting is active in the source database and downward if it has not been provisioned or is not active.
Needed	A check mark indicates that the policy is needed. An X indicates that the policy is not needed. If a policy that is not in use is set to needed, the In Use arrow points up after provisioning. If a policy that is in use is set to not needed, the audit policy is no longer displayed after provisioning. To select all policies as needed, click the Mark All as Needed button. To reverse this action, click Mark All as Not Needed .
(Rightmost column)	Click the trash can icon to remove the policy. You can use the trash can icon to remove the policy only if you had just created it and decided it was not required in the source database, or if it is not active in the source database.

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

Table 2–5 Fields in the Create Object Audit Page

Field	Description
Statements	Select the SQL statements to audit. To display a list of SQL statements for selection, click the flashlight icon. Examples are: <ul style="list-style-type: none"> ■ ALTER ■ AUDIT ■ UPDATE
Object Type	Select the type of object to audit, such as table. To display a list of object types and their audit sources for selection, click the flashlight icon. Examples are: <ul style="list-style-type: none"> ■ LOB ■ RULE ■ TABLE ■ VIEW

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

Field	Description
Object	Optional. Select the object to audit. To display a list of objects and their source databases for selection, and to filter the list by audit source and object owner, click the flashlight icon. For example, if you entered <code>TABLE</code> for the Object Type field, you could select <code>EMPLOYEES</code> , <code>JOBS</code> , or any of the other tables in the HR schema.
Statement Execution Condition	Choose the execution condition: <ul style="list-style-type: none"> ■ Both: Audits both successful and failed statements ■ Success: Audits the statement if it is successful ■ Failure: Audits the statement if it fails
DML Audit Granularity	Choose the level of granularity: <ul style="list-style-type: none"> ■ Access: Creates an audit record each time the operation occurs ■ Session: Creates an audit record the first time an operation occurs in the current session

2.6 Creating Oracle Audit Vault Policies for Privileges

This section contains:

- [About Privilege Auditing](#)
- [Defining a Privilege Audit Policy](#)

2.6.1 About Privilege Auditing

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

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

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

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

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

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

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

2.6.2 Defining a Privilege Audit Policy

To define a privilege audit policy:

1. If necessary, retrieve and activate the current privilege audit policies.
See [Section 2.3](#) for more information.
2. In the Audit Settings page, select the **Privilege** tab to display the Privilege page.
[Table 2–6](#) on page 2-11 describes the fields used in the Privilege page.
3. Click the **Create** button and in the Create Privilege Audit page, define the privilege audit policy.
[Table 2–7](#) on page 2-12 describes the Create Privilege Audit fields.
4. Click **OK**.

The privilege audit policy is created. To ensure that the privilege audit policy is semantically correct, see [Section 2.9](#).

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

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

[Table 2–6](#) lists the fields used in the Privilege page.

Table 2–6 Fields in the Privilege Page

Field	Description
(Leftmost column)	An exclamation mark icon indicates one of the following conditions: <ul style="list-style-type: none"> ■ The statement is needed but is not in use. ■ The statement is in use but is not needed.
Privilege	The privilege that is audited
User	The user to which this setting applies
Proxy User	The proxy user for the database, if any
Execution Condition	The execution condition audited: <code>WHENEVER SUCCESSFUL</code> , <code>WHENEVER NOT SUCCESSFUL</code> , or <code>BOTH</code>
Audit granularity	The granularity of auditing: <code>BY ACCESS</code> or <code>BY SESSION</code>
In Use	The arrow points upward if the setting is active in the source database and downward if it has not been provisioned or is not active.
Needed	A check mark indicates that the policy is needed. An X indicates that the policy is not needed. If a policy that is not in use is set to needed, the In Use arrow points up after provisioning. If a policy that is in use is set to not needed, the audit policy is no longer displayed after provisioning. To select all policies as needed, click the Mark All as Needed button. To reverse this action, click Mark All as Not Needed .

Table 2–6 (Cont.) Fields in the Privilege Page

Field	Description
(Rightmost column)	Click the trash can icon to remove the policy. You can use the trash can icon to remove the policy only if you had just created it and decided it was not required in the source database, or if it is not active in the source database.

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

Table 2–7 Fields in the Create Privilege Audit Page

Field	Description
Privilege	Select the privilege to audit. To display a list of privileges for selection, click the flashlight icon. Examples are: <ul style="list-style-type: none"> ■ ADMINISTER DATABASE TRIGGER ■ CREATE ANY TABLE ■ MANAGE TABLESPACE
Audited By	Choose the category of users to audit: <ul style="list-style-type: none"> ■ All: Audits all users, including proxy users. ■ User: Audits the user to which this setting applies. When you select this option, the Users field appears, in which you must specify at least one user. To display a list of users and their audit sources for selection, click the flashlight icon. ■ Proxy User: Audits the proxy user for the database. When you select this option, the Proxy User field appears, in which you must specify at least one user. To display a list of proxy users and their audit sources for selection, click the flashlight icon.
Statement Execution Condition	Choose the execution condition: <ul style="list-style-type: none"> ■ Both: Audits both successful and failed statements ■ Success: Audits the statement if it is successful ■ Failure: Audits the statement if it fails
DML Audit Granularity	Choose the level of granularity: <ul style="list-style-type: none"> ■ Access: Creates an audit record each time the operation occurs ■ Session: Creates an audit record the first time an operation occurs in the current session

2.7 Creating Oracle Audit Vault Policies for Fine-Grained Auditing

This section contains:

- [About Fine-Grained Auditing](#)
- [Defining a Fine-Grained Auditing Policy](#)

2.7.1 About Fine-Grained Auditing

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

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

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

2.7.1.1 Auditing Specific Columns and Rows

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

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

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

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

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

2.7.1.2 Using Event Handlers in Fine-Grained Auditing

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

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

2.7.2 Defining a Fine-Grained Auditing Policy

To define a fine-grained auditing policy:

1. If necessary, retrieve and activate the current fine-grained auditing policies.
See [Section 2.3](#) for more information.
2. In the Audit Settings page, select the **FGA** tab to display the FGA (fine-grained auditing) page.

The FGA page appears similar to the following:

Overview Statement Object Privilege FGA Capture Rule							
<input type="button" value="Mark All as Needed"/> <input type="button" value="Mark All as Not Needed"/> <input type="button" value="Create"/>							
Policy Name	Schema	Object	Statement	Columns	In Use	Needed	
EMPLOYEEEDATA	HR	EMPLOYEES	S, I, U, D	PHONE_NUMBER	↑	✓	
OE_ORDERS_TOTAL	OE	ORDERS	S, I, U, D	ORDER_TOTAL	↑	✓	
NONAPPSUSER	OE	ORDERS	S		↑	✓	
NONAPPSALES	SH	SALES	S, I, U, D		↑	✓	

[Table 2–8](#) on page 2-15 describes the fields used in the FGA page.

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

Create Fine Grained Audit

* Policy Name

* Audit Trail

* Object

* Statements

Columns

All
 Any

Condition

Handler Schema

Handler Package

Handler

[Table 2–9](#) on page 2-15 describes the Create Fine Grained Audit fields.

4. Click **OK**.

The fine-grained audit policy is created. To ensure that the fine-grained audit policy is semantically correct, see [Section 2.9](#).

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

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

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

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

Field	Description
(Leftmost column)	An exclamation mark icon indicates one of the following conditions: <ul style="list-style-type: none"> ■ The statement is needed but is not in use. ■ The statement is in use but is not needed.
Policy Name	The name of this fine-grained audit policy
Schema	The schema to which this policy applies
Object	The object to which this policy applies
Statement	The SQL statement to which this policy applies. Values are: <ul style="list-style-type: none"> ■ S: SELECT ■ I: INSERT ■ U: UPDATE ■ D: DELETE ■ M: MERGE
Columns	The database columns being audited, also referred to as the relevant columns. If this field is empty, all columns are audited.
In Use	The arrow points upward if the setting is active in the source database and downward if it has not been provisioned or is not active.
Needed	A check mark indicates that the policy is needed. An X indicates that the policy is not needed. If a policy that is not in use is set to needed, the In Use arrow points up after provisioning. If a policy that is in use is set to not needed, the audit policy is no longer displayed after provisioning. To select all policies as needed, click the Mark All as Needed button. To reverse this action, click Mark All as Not Needed .
(Rightmost column)	Click the trash can icon to remove the policy. You only can use the trash can icon to remove the policy if you had just created it and decided it was not required in the source database, or if it is not active in the source database.

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

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

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

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

Field	Description
Audit Trail	<p>Select from one of the following audit trail types:</p> <ul style="list-style-type: none"> ■ Database: Writes the policy records to the database audit trail <code>SYS.FGA_LOG\$</code> system table. ■ Database with SQL Text: Performs the same function as the Database option, but also populates the SQL bind and SQL text CLOB-type columns of the <code>SYS.FGA_LOG\$</code> table. ■ XML: Writes the policy records to an operating system XML file. To find the location of this file, a database administrator can run the following command in SQL*Plus: <pre>SQL> show parameter audit_file_dest</pre> ■ XML with SQL Text: Performs the same function as the XML option, but also includes all columns of the audit trail, including <code>SQLTEXT</code> and <code>SQLBIND</code> values. <p>Be aware that sensitive data, such as credit card numbers, appear in the audit trail if you collect SQL text.</p>
Object	<p>Select an object to audit (for example <code>OE.CUSTOMERS</code>). To display a list for selection and to filter objects by audit source, object owner, and object, click the flashlight icon.</p>
Statements	<p>Select one or more SQL statements to audit. To display a list of statements for selection, click the flashlight icon.</p> <p>Select from the following SQL statements:</p> <ul style="list-style-type: none"> ■ SELECT ■ INSERT ■ UPDATE ■ DELETE ■ MERGE
Columns	<p>Optional. Enter the names of the database columns (relevant columns) to audit. Separate each column name with a comma. If you enter more than one column, select All or Any as the condition that triggers this policy.</p> <p>For example, if you selected the <code>OE.CUSTOMERS</code> table, you could select these columns:</p> <pre>CUSTOMER_ID, CREDIT_LIMIT, DATE_OF_BIRTH</pre> <p>See Section 2.7.1.1 for more information about relevant columns.</p>
Condition	<p>Optional. Enter a Boolean condition to filter row data.</p> <p>For example:</p> <pre>department_id = 50</pre> <p>If this field is blank or null, auditing occurs regardless of condition.</p>
Handler Schema	<p>Mandatory if you specify an event handler. Enter the name of the schema account in which the event handler was created.</p> <p>For example:</p> <pre>SEC_MGR</pre> <p>See Section 2.7.1.2 for more information about event handlers.</p>

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

Field	Description
Handler Package	Mandatory if you specify an event handler. Enter the name of the package in which the event handler was created. For example: OE_FGA_POLICIES
Handler	Optional. Enter the name of the event handler. For example: CHECK_OE_VIOLATIONS If you specify an event handler, then you must specify its schema and package as well.

2.8 Creating Capture Rules for Redo Log File Auditing

This section contains:

- [About Capture Rules Redo Log File Auditing](#)
- [Defining a Capture Rule for Redo Log File Auditing](#)

2.8.1 About Capture Rules Redo Log File Auditing

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

In the source database, ensure that the table that you plan to use for the redo log file audit is not listed in the `DBA_STREAMS_UNSUPPORTED` data dictionary view. This is because the REDO collector uses Oracle Streams and Oracle LogMiner to read the redo logs. If there is a column type that is unsupported, then Oracle Audit Vault cannot extract the before and after values from the table.

2.8.2 Defining a Capture Rule for Redo Log File Auditing

To define a capture rule:

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

[Table 2–10](#) on page 2-18 describes the fields used in the Capture Rule page.
2. Click the **Create** button and in the Create Capture rule page, define the capture rule.

The screenshot shows the 'Create Capture Rule' dialog box. It has a title bar with the text 'Create Capture Rule' and two buttons: 'Cancel' and 'OK'. Below the title bar, there are four radio buttons: '* Capture Rule' (which is selected), 'Table', 'Schema', and 'Global'. Underneath these is a text input field with the label '* Table' and a help icon to its right. At the bottom of the dialog, there are four radio buttons: '* Capture' (selected), 'DDL', 'DML', and 'Both'.

Table 2–11 on page 2-19 describes the Create Capture Rule page fields.

3. Click **OK**.

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

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

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

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

Table 2–10 Fields in the Capture Rule Page

Field	Description
(Leftmost column)	An exclamation mark icon indicates one of the following conditions: <ul style="list-style-type: none"> ■ The statement is needed but is not in use. ■ The statement is in use but is not needed.
Rule Type	The types of capture rules are as follows: <ul style="list-style-type: none"> ■ Table: Captures or discards either row changes resulting from DML changes or DDL changes to a particular table. ■ Schema: Captures or discards either row changes resulting from DML changes or DDL changes to the database objects in a particular schema. ■ Global: Captures or discards either all row changes resulting from DML changes or all DDL changes in the database.
Schema	Indicates the schema to which this rule applies
Table	For table capture rules, this field indicates the table to which this rule applies.
DDL	YES or NO indicates whether data definition language (DDL) statements are audited.
DML	YES or NO indicates whether data manipulation language (DML) statements are audited.
In Use	The arrow points upward if the setting is active in the source database and downward if it has not been provisioned or is not active.
Needed	A check mark indicates that the policy is needed. An X indicates that the policy is not needed. If a policy that is not in use is set to needed, the In Use arrow points up after provisioning. If a policy that is in use is set to not needed, the audit policy is no longer displayed after provisioning. To select all policies as needed, click the Mark All as Needed button. To reverse this action, click Mark All as Not Needed .
(Rightmost column)	Click the trash can icon to remove the policy. You can use the trash can icon to remove the policy only if you had just created it and decided it was not required in the source database, or if it is not active in the source database.

[Table 2–11](#) lists the fields used in the Create Capture Rule page.

Table 2–11 Fields in the Create Capture Rule Page

Field	Description
Capture Rule	<p>Select from the following capture rule types:</p> <ul style="list-style-type: none"> ▪ Table: Captures either row changes resulting from DML changes or DDL changes to a particular table. The Table field appears; enter the name of the table to which the capture rule applies. To display a list of tables and their audit sources, and to filter by object owner and object, click the flashlight icon. ▪ Schema: Captures either row changes resulting from DML changes or DDL changes to the database objects in a particular schema. The Schema field appears; enter the name of the schema, or click the flashlight icon to select from a list. ▪ Global: Captures either all row changes resulting from DML changes or all DDL changes in the database.
Capture	<p>Select from the following:</p> <ul style="list-style-type: none"> ▪ DDL (data definition language) ▪ DML (data manipulation language) ▪ Both

2.9 Verifying Oracle Audit Vault Policy Settings

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

1. From within the Audit Vault Console, select the **Audit Policy** tab.
2. Under Audit Source, select the name of the source database.

The Apply Audit Settings section appears.

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

By default, all audit types are selected.

4. Under Apply Audit Settings, click the **Verify** button.

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

2.10 Provisioning Audit Vault Policies to the Source Oracle Database

After you have created, verified, and saved the audit policies, you can provision the audit policy changes to the source database. To verify that the audit policy changes have taken affect, you can retrieve a snapshot from the source database, as described in [Section 2.3.1](#).

You can provision the audit policy settings in the following ways:

- [Saving the Audit Policy Settings to a SQL Script for a Database Administrator](#)
- [Manually Provisioning the Audit Policy Settings to the Source Database](#)

Caution: Any audit policy that is not indicated as **Needed** in Audit Vault will be turned off on the source database. [Section 2.3.1](#) describes how to retrieve audit policies from a source Oracle database.

2.10.1 Saving the Audit Policy Settings to a SQL Script for a Database Administrator

To save the audit settings to a SQL script:

1. From within the Audit Vault Console, click the **Database Instance** link to display the Dashboard page.
2. Select the name of the source database.
The Apply Audit Settings section appears.
3. Select from the audit settings types the audit settings that you want to export: **Statement, Object, Privilege, FGA, or Capture Rule**.
By default, all the audit settings types are selected.
4. Click **Export as SQL** to save the settings to a SQL script. In the **Browse** dialog field, select a location for the SQL file.
5. Give this script to your database administrator, who can apply the policies to the source database.

2.10.2 Manually Provisioning the Audit Policy Settings to the Source Database

To manually provision the audit settings to the source database.

1. From within the Audit Vault Console, click the **Database Instance** link to display the Dashboard page.
2. Select the name of the source database.
The Apply Audit Settings section appears.
3. Select from the audit settings types the audit settings that you want to export: **Statement, Object, Privilege, FGA, or Capture Rule**.
By default, all the audit settings types are selected.
4. In the **Audit Source User Name** field, enter the user name of a user who has been granted the EXECUTE privilege for the AUDIT SQL statement, the NOAUDIT SQL statement, and the DBMS_FGA PL/SQL package.
If the source database is protected with Oracle Database Vault, ensure that the user has been granted the AUDIT SYSTEM and AUDIT ANY privileges. If there is an audit command rule in place, ensure the command is enabled and the user whose name you enter is able to execute the command.
5. In the **Audit Source Password** field, enter the password of this user.
6. Click the **Provision** button.

After you provision the audit settings to the source database, a database administrator can modify or delete audit policies. For this reason, you should periodically retrieve the settings to ensure that you have the latest audit settings. [Section 2.3](#) describes how to fetch audit settings.

2.11 Copying Oracle Audit Vault Policies to Other Oracle Databases

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

1. From within the Audit Vault Console, click the **Database Instance** link to display the Dashboard page.
2. Select the name of the source database.
The Apply Audit Settings section appears.
3. Select audit settings for types that you want to copy: **Statement, Object, Privilege, FGA, and Capture Rule**.
By default, all the audit settings types are selected.
4. In the **From** field under Copy Audit Settings from Another Source, enter the name of a source database that is different from the current source database, or use the flashlight icon to select it from a list.
5. After **Copy**, select either of the following options:
 - **Actual (In Use):** Copies the settings listed in the **In Use** field under Apply Audit Settings.
 - **Needed (Not Yet In Use):** Copies the settings listed in the **Needed** field under Apply Audit Settings.
6. In the **From** field, enter the full name of the source database from which you want to copy, or use the flashlight icon to select its name from a list.
You can filter the source databases by source name, host name, and host IP address.
7. Click the **Load** button.
8. Click the **Save All Audit Settings** button.
9. Export the settings to a SQL file or provision the settings to the source database, using the procedure described in [Section 2.10](#).

2.12 Creating and Configuring Alerts

This section contains:

- [About Alerts](#)
- [Creating Templates to be Used for Alerts](#)
- [Creating Alert Status Values](#)
- [Creating a Basic Alert](#)
- [Creating an Advanced Alert](#)
- [Monitoring Alerts](#)

2.12.1 About Alerts

You can create and configure alerts for Oracle Database, Microsoft SQL Server, Sybase ASE, and IBM DB2 source databases. The alert is raised when the incoming audit data

violates specific audit policies. You can specify an alert level and associate the alert with the events described in [Appendix A](#) through [Appendix D](#).

When an incoming audit record meets the specified condition, an alert is raised and placed in the alert store, where you can review and respond to it as necessary. For example, you may want to send an e-mail to a security officer or file a trouble ticket within the appropriate tracking system. You can configure templates to be used for this type of alert notification. [Section 2.13](#) describes how to respond to an alert.

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

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

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

2.12.2 Creating Templates to be Used for Alerts

This section contains:

- [About Notification Alert Templates](#)
- [Creating an E-Mail Notification Profile](#)
- [Creating an E-Mail Notification Template](#)
- [Creating a Trouble Ticket Template](#)

2.12.2.1 About Notification Alert Templates

You can configure Oracle Audit Vault alerts to trigger an e-mail in response to an Audit Vault alert being raised or a report being generated. For example, suppose you create an alert that is triggered every time a connection is made by an application shared schema account outside of the application (for example, APPS or SYSADM). When the user tries to log in, Oracle Audit Vault sends an e-mail to an administrator warning him or her of misuse of the application account. To accomplish this, you must create an e-mail notification profile that defines who will receive the e-mail, and then create an e-mail template that contains a message.

You also can create a trouble ticket that can be used log trouble tickets in response to an alert. Before you can do so, you must create a trouble ticket template.

2.12.2.2 Creating an E-Mail Notification Profile

The e-mail notification profile is a way of creating an e-mail group for a specific notification purpose, that is, a distribution list. For example, if you need to send e-mail to all auditors in your group, you can create an e-mail notification profile. When you create an alert, you can use this profile to specify an e-mail list of recipients.

To create a notification profile:

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

[Section 1.4](#) explains how to start the Audit Vault Console.

2. From the Dashboard page, select the **Settings** tab.
3. Select the **Notification Profiles** tab.
The Notification Profiles page is displayed by default. It displays a list of existing notification profiles, which you can modify or delete.
4. Click the **Create** button, and in the Add Notification Profile page, define the notification profile.

The screenshot shows the Oracle Enterprise Manager 10g Audit Vault interface. The top navigation bar includes 'Home', 'Audit Reports', 'Audit Policy', and 'Settings'. Below this, a sub-navigation bar highlights 'Notification Profiles'. The main content area is titled 'Add Notification Profile' and contains the following fields:

- Profile Name**: A required text input field.
- Description**: A text area for optional description.
- To**: A required text input field for email addresses.
- CC**: A text input field for additional email addresses.

Buttons for 'Cancel' and 'Save' are located at the top right of the form area.

Table 2–12 describes the Add Notification Profile fields.

5. Click the **Save** button.
After you create the profile, it is listed in the Profile List section of the Notification Profile. From there, you can modify or delete profiles as necessary.

Table 2–12 lists the fields used in the Add/Edit Notification Profile Page.

Table 2–12 Fields in the Add Notification Profile Page

Field	Description
Profile Name	Enter a name of the notification profile. For example: All Auditors
Description	Optionally, enter a description of the notification profile. For example: Profile used for notifications that are sent to all auditors
To	Enter a list of user or group e-mail addresses, each separated by a comma. For example: auditors_ca@example.com, sec_admin@example.com
CC	Optionally, include additional e-mail addresses if you want. For example: ida.neau@example.com, kari.uksa@example.com, nessa.sarie@example.com, ima.kuksa@example.com

2.12.2.3 Creating an E-Mail Notification Template

An e-mail notification template enables you to specify the content of the e-mail when you send it to other users, including the e-mail recipients specified in an e-mail notification template, when an Oracle Audit Vault alert is raised or an Audit Vault report is generated.

To create a notification template:

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

[Section 1.4](#) explains how to start the Audit Vault Console.

2. From the Dashboard page, select the **Settings** tab.
3. Select the **Notification Templates** tab.

The Notification Templates page displays a list of existing notification templates, which you can modify or delete. Some of these templates are predefined.

4. Click the **Create** button and in the Add Notification Template page, define a notification template.

[Table 2–13](#) describes the Add Notification Template page.

5. Click **Save**.

After you create the template, it is listed in the Notification Templates page. From there, you can modify or delete templates as necessary.

Table 2–13 lists the fields used in the Add Notification Template page.

Table 2–13 Fields in the Add Notification Template Page

Field	Description
Type	Specify the type of notification. Select from the following options: <ul style="list-style-type: none"> ■ Alert: Creates a notification template used by the alerts. ■ Report Attachment: Attaches a PDF of the audit report to the e-mail notification. ■ Report Notification: Creates a notification template used by reports, but does not attach the PDF file of the report.
Name	Enter a name for the template. For example: Critical Alert E-Mail for non-os User Access Attempts
Description	Enter a brief description of what the template will be used for. For example: Alerts admins if non-OS users try to log into the database
Subject	Enter a subject header for the alert. You can use the supplied tags to provide dynamic text based on the content of the alert or report. For example: #AlertSeverity# Alert: Non-OS User Trying to Access the employee_db Database #Date_created#
Format	Select either Plain Text or HTML .
Body	Enter the body text for the notification. You can use the tags listed under Available Tags to associate existing alerts with the notification. Table 2–14 and Table 2–15 describe these tags in detail. For example, suppose you create the following body text for an alert notification: The "#Report_name#", generated on #Date_created#, is ready for your review. You can review the report at the following location: #URL# Please do not reply to this e-mail. This is an automatically generated message. The generated message could, depending on the circumstances and alert generated, say something similar to the following: The System Privileges Report, generated on Sept 26, 2009, 3:15:06 PM, is ready for your review. You can review the report at the following location: http://mau.example.com:5707/av/console/f?p=7700:4:3525486105242281::NO::P4_REPORT_ID:36 Please do not reply to this e-mail. This is an automatically generated message.

Table 2–14 lists the available tags for alert notifications.

Table 2–14 Notification Template Alert Tags

Alert Tag Name	Description
#AlertName#	Name of the alert
#AlertTime#	Time the event causing the alert was created
#AlertStatus#	Status of the Alert (for example, New , Open , or Closed)
#Object#	Schema name and object name from the event that caused the alert
#AlertSeverity#	Severity of the alert (Critical or Warning)

Table 2–14 (Cont.) Notification Template Alert Tags

Alert Tag Name	Description
#ClientHost#	Host name of the client
#ClientHostIP#	IP address of the client
#Event#	Audit event (for example, DELETE for a data access event). See the following appendixes for more information about audit events: <ul style="list-style-type: none"> ■ Appendix A, "Oracle Database Audit Events" ■ Appendix B, "Microsoft SQL Server Audit Events" ■ Appendix C, "Sybase Adaptive Server Enterprise Audit Events" ■ Appendix D, "IBM DB2 Audit Events"
#OSUserName#	The operating system user name associated with the event
#UserName#	The user name associated with the event (a database event because Oracle Audit Vault currently collects only database events)
#SourceName#	Source database in which the alert was raised.
#Description#	Description of the alert
#TroubleTicketID#	The trouble ticket ID that has been created for this alert
#TroubleTicketTime#	The time the trouble ticker has been created
#URL#	URL of the alert
#AlertBody#	A special tag that is a shortcut to include the following fields in the e-mail: Alert Name, Alert Time, Alert Status, Object, Alert Severity, Client Host, Client Host IP, Event, OS User Name, User Name, Source Name, Description, Trouble Ticket ID, Trouble Ticket Time, and URL

Table 2–15 lists the available tags for report notifications.

Table 2–15 Notification Template Report Tags

Report Tag Name	Description
#ReportName#	Name of the report
#DateCreated#	Date and time the alert was generated
#ReportCategory#	Event category for the report (for example, data access event). See the following appendixes for more information about audit event categories: <ul style="list-style-type: none"> ■ Appendix A, "Oracle Database Audit Events" ■ Appendix B, "Microsoft SQL Server Audit Events" ■ Appendix C, "Sybase Adaptive Server Enterprise Audit Events" ■ Appendix D, "IBM DB2 Audit Events"
#URL#	URL to the report that was generated

2.12.2.4 Creating a Trouble Ticket Template

A trouble ticket template is a form that defines a trouble ticket action that must be logged in response to an alert.

To create a trouble ticket template:

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

[Section 1.4](#) explains how to start the Audit Vault Console.

2. From the Dashboard page, select the **Settings** tab.
3. Select the **Trouble Ticket Templates** tab.

The Trouble Ticket Templates page displays a list of existing trouble ticket templates, which you can modify or delete.

4. Click the **Create** button and in the Add Trouble Ticket Template page, define the template.

Add Trouble Ticket Template Cancel Save

Please provide the data for all required fields.

* Template Name

Description

* Assigned Support Group

* Assigned Support Company

* Assigned Support Org

* First Name

* Last Name

* Summary

* Notes

* Critical level Alert

* Warning level Alert

Available Tags

- #AlertName#
- #AlertTime#
- #AlertStatus#
- #Object#
- #AlertSeverity#
- #Client-Host#
- #Client-HostIP#
- #Event#
- #OSUserName#
- #UserName#
- #SourceName#
- #Description#
- #TroubleTicketID#
- #TroubleTicketTime#
- #URL#
- #AlertBody#

[Table 2-16](#) lists the fields used in the Trouble Ticket Template page.

5. Click **Save**.

After you create the template, it is listed in the Trouble Ticket Templates page. From there, you can modify or delete templates as necessary.

[Table 2-16](#) lists the fields used in the Trouble Ticket Template page.

Table 2-16 Fields Used in the Add Trouble Ticket Template Page

Field	Description
Template Name	Enter a name for the trouble ticket template. For example: hr_data_tmpl
Description	Optionally, enter a description for the trouble ticket template. For example: Template to be used for any HR data violations

Table 2–16 (Cont.) Fields Used in the Add Trouble Ticket Template Page

Field	Description
Assigned Support Group	<p>Enter the name of the support group that is assigned the trouble ticket. Check with your Remedy administrator for the value to be used. For example:</p> <p>sec_support</p>
Assigned Support Company	<p>Enter the name of the company that is assigned the trouble ticket. Check with your Remedy administrator for the value to be used. For example:</p> <p>Example, Inc.</p>
Assigned Support Org	<p>Enter the name of the support organization that is assigned to the trouble ticket. Check with your Remedy administrator for the value to be used. For example:</p> <p>sec_support_org</p>
First Name	<p>Enter the first name of the customer for whom you are creating the trouble ticket. Check with your Remedy administrator for the value to be used. For example:</p> <p>Ima</p>
Last Name	<p>Enter the last name of the customer. Check with your Remedy administrator for the value to be used. For example:</p> <p>Noyd</p>
Summary	<p>Enter a detailed summary of the trouble ticket incident. You can use the tags listed under Available Tags to associate existing alerts with the trouble ticket template. Table 2–15 on page 2-26 describes these tags in detail.</p> <p>For example, suppose you enter the following text:</p> <pre>#ReportName# was generated on #DateCreated#. Please see the following URL: #URL#</pre> <p>In the trouble ticket, depending on the circumstances, it could appear as follows:</p> <p>The Data Access Report was generated on Sept 30, 2009, 3:15:06 PM. Please see the following URL:</p> <pre>http://mau.example.com:5707/av/console/f?p=7700:4:3525486105242281::NO::P4_REPORT_ID:58</pre>
Notes	<p>Enter notes for this ticket. For example:</p> <p>I think someone has been tampering with HR files again.</p>
Critical level Alert	<p>Select from the following levels:</p> <ul style="list-style-type: none"> ■ 1-Critical ■ 2-High (default) ■ 3-Medium ■ 4-Low <p>These levels categorize the alert only.</p>

Table 2–16 (Cont.) Fields Used in the Add Trouble Ticket Template Page

Field	Description
Warning level Alert	Select from the following levels: <ul style="list-style-type: none"> ■ 1-Critical ■ 2-High ■ 3-Medium (default) ■ 4-Low <p>These levels categorize the alert only.</p>

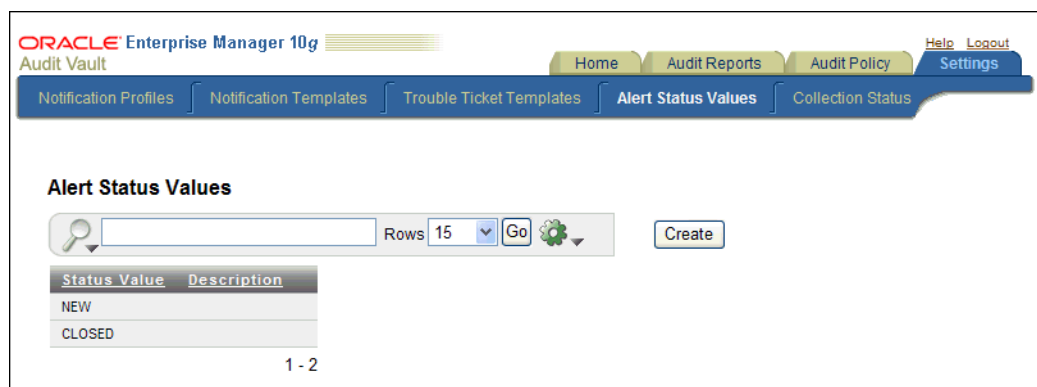
2.12.3 Creating Alert Status Values

You can create alert status values to assign to an alert during the lifetime of the alert. Oracle Audit Vault provides two status values: `NEW` and `CLOSED`. You can create additional ones to suit your needs, such as `PENDING`.

To create an alert status value:

1. Log in to the Audit Vault Console as a user who has been granted the `AV_AUDITOR` role.
[Section 1.4](#) explains how to start the Audit Vault Console.
2. In the Audit Vault Console, select the **Settings** tab, and then select the **Alert Status Values** secondary tab.

The Alert Status Values page appears.



3. To create a new alert status, click the **Create** button.

The Add Alert Status Value page appears.

4. Enter the following settings:
 - **Status Value:** Enter a name for the status value (for example, `PENDING`).
 - **Description:** Optionally, enter a description for the status value. For example:
Use this value to assign to alerts that are in process of being resolved and have not yet been closed.
5. Click the **Save** button.

The new alert status appears in the Alert Status Values page. From there, you can edit the alert status. To delete it, click the trash icon.

2.12.4 Creating a Basic Alert

A basic alert specifies a user, table, audit event, success criteria, and notification settings. For example, you could create a basic alert to be raised each time User X tries to modify Table Y.

To create a basic alert:

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

Section 1.4 explains how to start the Audit Vault Console.

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

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

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

3. Click **Create**.

The Create Alert Rule page appears.

4. In the **Alert** field, enter the alert name and then in the **Description** field, enter a brief description of the alert.
5. Specify the following information:
 - **Alert Severity:** Select **Warning** or **Critical**.
 - **Audit Source Type:** Select one of the following audit source types:
 - **SYBDB** (for Sybase Adaptive Server Enterprise)
 - **MSSQLDB** (for Microsoft SQL Server)
 - **ORCLDB** (for Oracle Database)
 - **DB2DB** (for IBM DB2)

- **Audit Source:** Select from the list of source databases based on the audit source type that you selected.
 - **Audit Event Category:** Select from the list of available categories based on the audit source type that you selected. For detailed information about the audit events for these categories, see the following appendixes:
 - [Appendix A, "Oracle Database Audit Events"](#)
 - [Appendix B, "Microsoft SQL Server Audit Events"](#)
 - [Appendix C, "Sybase Adaptive Server Enterprise Audit Events"](#)
 - [Appendix D, "IBM DB2 Audit Events"](#)
6. After Specify additional alert conditions in, select **Basic**.

The following area appears on the Alerts page:

Specify additional alert conditions in Basic Advanced

Basic Alert Condition
Specify when an alert should be raised.

User

Table

Audit Event -- No Event --

* Audit Event Status Success Failure Both

7. Specify the following information:
- **User:** Specify the name of one or more users or click the flashlight icon to search for and select user names.

Oracle Audit Vault only lists the tables from the Oracle databases that have been configured for Audit Vault and since the last retrieve of the audit policy settings. To retrieve the latest audit policy settings, see [Section 2.3](#).
 - **Table:** Specify the name of one or more tables or click the flashlight icon to search for and select table names.

Oracle Audit Vault only lists the tables from the Oracle databases that have been configured for Audit Vault and since the last retrieve of the audit policy settings.
 - **Audit Event:** Select the name of an audit event from the list. The audit events that appear are based on the audit event category that you selected. See the following appendixes for more information about audit events:
 - [Appendix A, "Oracle Database Audit Events"](#)
 - [Appendix B, "Microsoft SQL Server Audit Events"](#)
 - [Appendix C, "Sybase Adaptive Server Enterprise Audit Events"](#)
 - [Appendix D, "IBM DB2 Audit Events"](#)
 - **Audit Event Status:** Select an option to represent whether the event has a status of **Success**, **Failure**, or **Both**.
8. Under Notification Action, optionally specify the following information:

Alert Action
When an alert is raised, take the following actions.

Notification Action

* Template: Profile:

To: Cc:

Profile Name	To	Cc	Template Name	Delete
av_auditors_distribution_list	idaneau@example.com, imaravin@example.com		Alert Notification Template	

Trouble Ticket Action

* Template:

- **Template:** From the list, select a notification template.
 - **Profile:** From the list, select a profile template.
 - **To:** Enter one or more e-mail addresses, each separated by a comma.
 - **Cc:** Enter one or more e-mail addresses, each separated by a comma.
 - **Add to List:** Click the Add to List button to record the e-mail recipients that you entered in the **To** and **Cc** fields.
9. Under Trouble Ticket Action, from the list, optionally select a trouble ticket template.
10. Click **OK**.

After you create the basic alert, you can modify all the fields of the alert except for the following fields:

- Alert Severity
- Audit Source Type
- Audit Source
- Audit Event Category

In addition, you can monitor the alert activity from the Dashboard page. See [Section 2.12.6](#) for more information.

2.12.5 Creating an Advanced Alert

This section contains:

- [About Advanced Alerts](#)
- [Creating an Advanced Alert That Uses a Condition](#)
- [Creating an Advanced Alert Condition That Uses a Function](#)

2.12.5.1 About Advanced Alerts

In the Advanced Alert Condition section of the Create Alert Rule page, you can construct a Boolean condition that evaluates audit event behavior. When the Boolean condition evaluates to `TRUE`, then Oracle Audit Vault raises the alert, and either notifies other users or creates a trouble ticket. The alert condition can be simple or complex. As a general guideline, try to keep your alert conditions simple. Overly complex conditions can slow the Audit Vault Server database performance.

The syntax for the alert condition is as follows:

```
audit_field operator expression
```

When you insert the audit event fields for the expression, Oracle Audit Vault encloses them in # (pound) symbols. For example:

- #USERNAME#
- #HOST_IP#
- #EVENT_STATUS#

See the event attributes tables in [Appendix A](#) through [Appendix D](#) for a full listing of the event attributes for the Oracle Database, SQL Server, Sybase ASE, and IBM DB2 source databases.

You can use any legal SQL function. For example:

- upper()
- lower()
- to_char()

You can use any legal SQL operator. For example:

- not
- like
- <
- >
- in
- and
- null

When using operators, follow these guidelines:

- Remember that Oracle Audit Vault evaluates an alert condition for each incoming audit record.
- You cannot use nested queries (for example, `not in SELECT...`) in the condition.

Wildcards are as follows:

- % (to match zero or more characters)
- _ (to match exactly one character)

You can group components within the condition by using parentheses. For example:

```
((A > B) and (B > C)) or C > D
```

You can create a user-defined function that retrieves data from a table for the alert evaluation. [Section 2.12.5.3](#).

2.12.5.2 Creating an Advanced Alert That Uses a Condition

To create an advanced alert:

1. Follow Step 1 through Step 5 in [Section 2.12.4](#).
2. After Specify additional alert conditions in, select **Advanced**.

The following area appears on the Alerts page:

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

0 of 2000

Select an event to insert it in the condition

Select an attribute to insert it in the condition

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

The event appears in the **Condition** field with its associated source event. For example, suppose you wanted to monitor application shared schema accounts that are being used outside the database. An example of this scenario is when the database user is APPS and the client identifier is set to NULL. From the **Audit Event Category** list, you would select **USER SESSION**. Then from the **Select an event to insert it in the condition** list, you select **LOGON**. Oracle Audit Vault then adds the following event code for logons to the **Condition** field:

```
#SOURCE_EVENTID# = '100'
```

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

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

For this example, you select **USERNAME**, which Oracle Audit Vault adds to the **Condition** field. At this stage, the **Condition** field appears as follows:

```
#SOURCE_EVENTID# = '100' #USERNAME#
```

Do not remove the # symbols that enclose the event code or the attribute.

- Modify the condition to build the expression.

For example:

```
#SOURCE_EVENTID# ='100'and lower (#USERNAME#) = 'apps' and #CLIENT_ID" = null
```

This alert says, "Raise an error if any ex-employee tries to log in to the database."

- Under Notification Action, optionally specify the following information:

- **Template:** From the list, select a notification template.
- **Profile:** From the list, select a profile template.
- **To:** Enter one or more e-mail addresses, each separated by a comma.
- **Cc:** Enter one or more e-mail addresses, each separated by a comma.
- **Add to List:** Click **Add to List** to create a listing of existing notification recipients, which will be listed

- Under Trouble Ticket Action, from the list, optionally select a trouble ticket template.

- Click **OK**.

2.12.5.3 Creating an Advanced Alert Condition That Uses a Function

You can create a function (or a package containing a set of functions) to use with the alert condition. For example, if the alert condition must test for a specific host name, then you can create a function that checks the host names listed in a table. This function can be used for any of the supported source database types.

Follow these guidelines when you create a table and function to use with an alert condition:

- Create the function and table on the Audit Vault Server database. The function and table should reside in the schema of the user who creates them.
- The user who creates the function and table must have the following privileges:
 - CREATE TABLE
 - CREATE PROCEDURE

In addition, ensure that this user has enough space to create the table and procedure in his or her tablespace, which by default is `USERS`. For example:

```
SQL> ALTER USER HOSTCHECKER QUOTA 10M ON USERS;
```

- The return type for the function can be any legal type, such as `CHAR`, `VARCHAR2`, or `NUMBER`. However, you cannot have a Boolean return type.
- You must grant the `EXECUTE` privilege for the function to the `AVREPORTUSER` account. This is a default user account that is designed to manage the Audit Vault reports.
- If the function is modified in the future or the function privileges changed, then the alert becomes invalid and does not work. Furthermore, the other alerts that were created for the alert category and source database (for example, all alerts created for the Account Management category for Oracle source databases) may not work as well. If this problem occurs, then check and correct the alert functions and privileges. Then drop and recreate the alert to use the corrected function. Afterward, all alerts created for the affected alert category and source database should work. Work with your Oracle Audit Vault administrator to troubleshoot alert issues.

To accomplish this, follow these general steps:

1. Log in to SQL*Plus in the Audit Vault Server database as the user responsible for creating the alert table and function.

For example:

```
$ sqlplus hostChecker
Enter password: password
Connected.
```

2. Create a table that contains the data that the function will retrieve.

For example:

```
SQL> CREATE TABLE hostlist (hostname VARCHAR2(100));
```

3. Create the function.

For example, to create a function that retrieves the host names populated in the `hostlist` table:

```
CREATE OR REPLACE FUNCTION checkhost (host IN VARCHAR2)
RETURN CHAR AS
```

```

        hostcount NUMBER;
BEGIN
    SELECT COUNT(*) INTO hostcount FROM hostchecker.hostlist WHERE LOWER(host) =
hostname;
    IF (hostcount > 0) THEN
        RETURN 'Y';
    ELSE
        RETURN 'N';
    END IF;
END checkhost;
/

```

4. Grant the EXECUTE privilege to the AVREPORTUSER user account.

For example:

```
SQL> GRANT EXECUTE ON CHECKHOST TO AVREPORTUSER;
```

Grant succeeded.

5. Create the advanced alert as described in [Section 2.12.5.2](#).

For example, the alert condition can be as follows:

```
hostChecker.checkHost (#HOST_NAME#) = 'N'
```

If you have not created the function properly, then Oracle Audit Vault prevents you from creating an alert to use the function. If this happens, check the structure of the alert and ensure that you have granted the AVREPORTUSER account the EXECUTE privilege for the function.

2.12.6 Monitoring Alerts

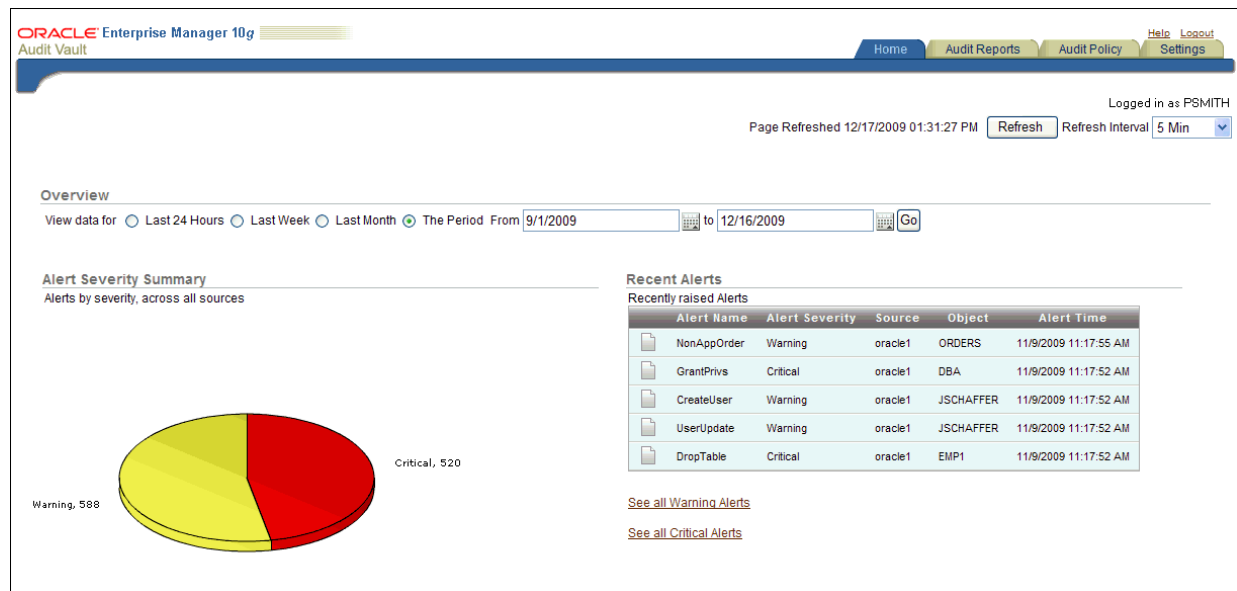
The **Overview** page is where auditors can view alert summaries, drill down to reports, and view agent and collector status. To display the Dashboard page, select the **Home** tab.

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

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

Figure 2–1 shows the a partial view of the Dashboard page.

Figure 2–1 Dashboard Page



From the Dashboard page, you can:

- Select an event start time and end time for viewing Audit Vault event data. You can specify a time period by month, week, or day time span or the period between a specified begin and end date.
- View five types of graphical summaries (pie charts and bar graphs) of alert activity and event activity over the specified time period. These graphical summaries include:
 - **Alert Severity Summary** (pie chart)
Click a section in this pie chart to drill down to a more detailed critical or warning alert report to see what sources are showing a particular severity level. See [Section 3.5](#) for more information about critical and warning alert reports.
 - **Summary of Alert Activity** (pie chart)
Click a section in this pie chart to find critical and warning alerts to see the affected sources for all alert activity.
 - **Top Five Audit Sources by Number of Alerts** (bar graph)
Click a bar in this bar graph to find more detailed critical and warning alert information that shows a severity level for a particular source.
 - **Alerts by Audit Event Category** frequency (number of alerts) (bar graph)
Click an event category link in this bar graph to drill down to see more detailed critical and warning alert information that shows all alerts for that event category.
 - **Activity by Audit Event Category** frequency (number of events) (bar graph)
Click an event category link in this bar graph to find events for that event category. You can generate default reports for these event categories. See [Chapter 3, "Using Oracle Audit Vault Reports"](#) for more information.

- Click a pie section or bar chart y-axis event category label to drill down to a more detailed report level.

2.13 Responding to an Alert

After you have created alerts and when they are generated, you or other auditors can respond to them. You can change the alert status (for example, closing it), notify other users of the alert, or log a trouble ticket for the alert.

To respond to an alert:

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

[Section 1.4](#) explains how to start the Audit Vault Console. The Dashboard page appears.
- Access the alert by using one of the following methods:
 - From the Dashboard page, select the alert from the **Recent Alerts** list.
 - From the Dashboard page, select the **See All Warning Alerts** link to access warning alerts.
 - From the Dashboard page, select the **See All Critical Alerts** link to access critical alerts.
 - Select the **Audit Report** tab, then the **Default Reports** secondary tab. Under Alert Reports, select either **All Alerts**, **Critical Alerts**, or **Warning Alerts**. Click **Go** to filter the report display.

The All Alerts page appears similar to following:

All Alerts

Set Status to **CLOSED**

Rows **15**

Audit Vault Alert Time is in the last 24 hours

Select	Details	Alert Name	Object	Event	Event Category	User	Source	Alert Severity	Event Time
<input type="checkbox"/>		NonAppOrder	ORDERS	SELECT	DATA ACCESS	OE	oracle1	Warning	9/22/2009 07:49:13 AM
<input type="checkbox"/>		UserUpdate	JSCHAFFER	CREATE USER	ACCOUNT MANAGEMENT	FRIPON	oracle1	Warning	9/22/2009 07:49:9 AM
<input type="checkbox"/>		CreateUser	JSCHAFFER	CREATE USER	ACCOUNT MANAGEMENT	FRIPON	oracle1	Warning	9/22/2009 07:49:9 AM
<input type="checkbox"/>		GrantPrivs	DBA	GRANT ROLE	ROLE AND PRIVILEGE MANAGEMENT	MALOEUF	oracle1	Critical	9/22/2009 07:49:9 AM
<input type="checkbox"/>		DropTable	EMP2	DROP TABLE	OBJECT MANAGEMENT	FRIPON	oracle1	Critical	9/22/2009 07:49:8 AM

- In the All Alerts page, select the check boxes for the reports to which you want to respond.
- Perform any of the following actions:
 - Notify another auditor of the alert.** Click the **Notify** button. In the Manual Alert Notification page, select the notification template and profile that you want to use, and optionally enter e-mail addresses in the **To** and **Cc** fields. Separate multiple e-mail addresses with a comma. Click the **Add to List** button to compile the listing, and then click the **Notify** button to send the notification.

- **Log a trouble ticket.** Click the **Log Trouble Tickets** button. In the Manual Trouble Ticketing page, select the trouble ticket template that you want from the **Template** list. Then click **OK**. The Alerts page appears, with a message describing the status (for example, *Successfully queued the trouble ticket logging request*).
- **Details.** Select the page icon under the **Details** column for the report, and under the Notes area, select either **Current Note** or **Previous Notes** to update the status of the alert, or log or update a Remedy ticket.

This method also enables you to file notification and trouble ticket information.
- **Set the alert status.** From the **Set Status to** list, select either **NEW** or **CLOSED**, and then click the **Apply** button. When an alert is first generated, it is set to **OPEN**. The Alerts page displays a message describing the status (for example, *Successfully updated the alert statuses*).

2.14 Setting a Retention Period for Audit Data

You can set a period of 1 to 99 years for Oracle Audit Vault to retain audit data. By default, Oracle Audit Vault retains collected audit data for 10 years. When you set this retention period, it applies to audit records from *all* source databases, not just the currently selected source database. Oracle Audit Vault deletes the data based on the time that it was collected by Oracle Audit Vault, not when the audit event actually occurred. For example, suppose you load audit data that is more than 10 years old and then you set the retention period to 7 years. Oracle Audit Vault will delete this audit data 7 years from now.

To set the audit data retention period:

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

[Section 1.4](#) explains how to start the Audit Vault Console. The Dashboard page appears.
2. In the Audit Vault Console, select the **Audit Policy** tab.

By default, the Audit Settings page appears.
3. Under Audit Data Retention, enter a value (1–99) in the **Retain audit data** field.
4. Click **Go**.

Using Oracle Audit Vault Reports

This chapter contains:

- [What Are Oracle Audit Vault Reports?](#)
- [Accessing the Oracle Audit Vault Audit Reports](#)
- [Using the Default Reports](#)
- [Using the Compliance Reports](#)
- [Using the Critical and Warning Alert Reports](#)
- [Scheduling and Creating PDF Reports](#)
- [Annotating and Attesting Reports](#)
- [Generating and Comparing Snapshots of Entitlement Audit Data](#)
- [Controlling the Display of Data in a Report](#)
- [Finding Information About Report Data](#)
- [Working with User-Defined Reports](#)
- [Downloading a Report to a CSV File](#)

3.1 What Are Oracle Audit Vault Reports?

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

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

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

3.2 Accessing the Oracle Audit Vault Audit Reports

To access the Oracle Audit Vault audit reports:

1. Log in to the Oracle Audit Vault Console as a user who has been granted the AV_AUDITOR role, as explained in [Section 1.4](#).

The Dashboard page appears.

2. Click the **Audit Reports** tab in the upper-right corner of the window.
3. Do one of the following:
 - **To view and work with reports:** Click the appropriate secondary tab to find the report you want to view (**Default Reports**, **Compliance Reports**, **Custom Reports**, or **Generated Reports**). To view the report (for example, Data Access under the Access Reports category), click its link.
 - **To schedule and send to another user a PDF report:** Click the **Report Schedules** secondary tab. See [Section 3.6](#).
 - **To annotate and attest a report:** Click the Generated Reports secondary tab, select the report, and then click the **Details** button. See [Section 3.7](#).
 - **To view snapshots of audit data in the entitlement reports:** Click **Entitlement Snapshots** secondary tab. See [Section 3.8](#).

3.3 Using the Default Reports

This section contains:

- [About the Default Reports](#)
- [Using the Default Access Reports](#)
- [Using the Default Management Activity Reports](#)
- [Using the Default System Exception Reports](#)
- [Using the Default Entitlement Reports](#)

3.3.1 About the Default Reports

The default reports are predefined reports that cover commonly required audit data.

Figure 3–1 shows the Default Reports page.

Figure 3–1 Default Reports Page



3.3.2 Using the Default Access Reports

This section contains:

- [About the Default Access Reports](#)
- [Activity Overview Report](#)
- [Data Access Report](#)
- [Database Vault Report](#)
- [Distributed Database Report](#)
- [Procedure Executions Report](#)
- [User Sessions Report](#)

3.3.2.1 About the Default Access Reports

The default access reports track general database access activities such as audited SQL statements, Oracle Database Vault activities, application access activities, and user login activities. These reports display the following kinds of information: source database name, source database type, host name for the source database, version of the source database, IP address of the source database, audit time, Audit Vault category, the event itself (such as `LOGIN` statements), current and previous values of the event, user and host client information, the event status (such as failure), and the time the event took place.

You can create user-defined custom reports from the reports. See [Section 3.9](#) and [Section 3.11](#).

3.3.2.2 Activity Overview Report

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

If you suspect that the Audit Vault data warehouse is not being refreshed with the latest audit data, then check the Activity Overview Report. If you find that the audit data that you want is not listed in this report, then ask your Audit Vault administrator to check the server-side log files (alert and trace logs) for errors. If there are errors, then contact Oracle Support.

Figure 3–2 shows the Activity Dashboard page.

Figure 3–2 Activity Overview Report Page

Source	Category	Event	User	Target	Host	Event Time
oracle1	USER SESSION	LOGOFF	MALOEUF		binks241	10/16/2009 05:11:12 PM
oracle1	USER SESSION	LOGOFF	MALOEUF		binks241	10/16/2009 05:11:8 PM
oracle1	USER SESSION	LOGOFF	MALOEUF		binks241	10/16/2009 05:9:35 PM
oracle1	USER SESSION	LOGOFF	MALOEUF		binks241	10/16/2009 08:30:55 AM
oracle1	USER SESSION	LOGOFF	MALOEUF		binks241	10/15/2009 09:28:6 PM
oracle1	USER SESSION	LOGOFF	MALOEUF		binks241	10/15/2009 11:23:33 AM
oracle1	USER SESSION	LOGOFF	MALOEUF		binks241	10/15/2009 11:19:53 AM
oracle1	SYSTEM MANAGEMENT	SUPER USER DML	/			10/13/2009 03:58:21 PM
oracle1	USER SESSION	SUPER USER LOGON	/			10/13/2009 03:57:49 PM
oracle1	USER SESSION	LOGOFF	MALOEUF		binks241	10/8/2009 08:16:50 PM
oracle1	USER SESSION	LOGOFF	MALOEUF		binks241	10/7/2009 07:40:49 AM
oracle1	USER SESSION	LOGOFF	MALOEUF		binks241	10/6/2009 04:13:51 PM
oracle1	USER SESSION	LOGOFF	MALOEUF		binks241	10/6/2009 01:9:55 PM
oracle1	USER SESSION	LOGOFF	MALOEUF		binks241	10/6/2009 12:12:24 PM
oracle1	SYSTEM MANAGEMENT	SUPER USER DDL	/			10/6/2009 10:59:52 AM

3.3.2.3 Data Access Report

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

See Also:

- [Section A.5](#) for Oracle Database audit events
- [Section B.5](#) for SQL Server audit events
- [Section C.5](#) for Sybase Adaptive Server Enterprise audit events
- [Section D.5](#) for IBM DB2 audit events
- [Section 3.4.5.9](#) if you want to use the Program Change Report to track changes to row data from INSERT or UPDATE statements

3.3.2.4 Database Vault Report

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

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

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

PARAMETER	VALUE
Oracle Database Vault	TRUE

See also [Section A.6](#) for a listing of the Oracle Database Vault audit events.

3.3.2.5 Distributed Database Report

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

See Also:

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

3.3.2.6 Procedure Executions Report

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

See Also:

- [Section A.12](#) for Oracle Database audit events
- [Section B.11](#) for SQL Server audit events
- [Section C.11](#) for Sybase Adaptive Server Enterprise audit events
- [Section D.11](#) for IBM DB2 audit events
- [Section 3.3.3.5](#) for information about the Procedure Management Report

3.3.2.7 User Sessions Report

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

See Also:

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

3.3.3 Using the Default Management Activity Reports

This section contains:

- [About the Default Management Activity Reports](#)
- [Account Management Report](#)
- [Audit Commands Report](#)
- [Object Management Report](#)
- [Procedure Management Report](#)
- [Role and Privilege Management Report](#)
- [System Management Report](#)

3.3.3.1 About the Default Management Activity Reports

The default management activity reports track the use of `AUDIT SQL` statements, changes to user accounts, actions performed on the underlying packages for applications, actions performed on database objects, roles and privileges, and system management activities such as database shutdowns and startups. These reports display the following kinds of information: source database name, source database type, host name for the source database, version of the source database, IP address of the source database, audit time, Audit Vault category, the event itself (such as `GRANT` statements), current and previous values of the event, user and host client information, the event status (such as failure), and the time the event took place.

You can create user-defined reports from the reports. See [Section 3.9](#) and [Section 3.11](#).

3.3.3.2 Account Management Report

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

See Also:

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

3.3.3.3 Audit Commands Report

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

See Also:

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

3.3.3.4 Object Management Report

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

See Also:

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

3.3.3.5 Procedure Management Report

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

See Also:

- [Section A.3](#) for Oracle Database audit events
- [Section B.3](#) for SQL Server audit events
- [Section C.3](#) for Sybase Adaptive Server Enterprise audit events
- [Section D.3](#) for IBM DB2 audit events
- [Section 3.3.2.6](#) for information about the Procedure Executions Report

3.3.3.6 Role and Privilege Management Report

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

See Also:

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

3.3.3.7 System Management Report

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

See Also:

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

3.3.4 Using the Default System Exception Reports

This section contains:

- [About the Default System Exception Reports](#)
- [Exception Activity Report](#)
- [Invalid Audit Record Report](#)
- [Uncategorized Activity Report](#)

3.3.4.1 About the Default System Exception Reports

The default system exception reports track audit events, such as exceptions that occur and audit activities that Oracle Audit Vault cannot recognize or place into a category. These reports display the following kinds of information: source database name, source database type, host name for the source database, version of the source database, IP address of the source database, audit time, Audit Vault category, the event itself (such as network errors), current and previous values of the event, user and host client information, the event status (such as failure), and the time the event took place. You can create user-defined reports from the reports. See [Section 3.9](#) and [Section 3.11](#).

3.3.4.2 Exception Activity Report

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

See Also:

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

3.3.4.3 Invalid Audit Record Report

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

See Also:

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

3.3.4.4 Uncategorized Activity Report

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

See Also:

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

3.3.5 Using the Default Entitlement Reports

This section contains:

- [About the Default Entitlement Reports](#)
- [User Accounts Report and User Accounts by Source Report](#)
- [User Privileges Report and User Privileges by Source Report](#)
- [User Profiles Report and User Profiles by Source Report](#)
- [Database Roles Report and Database Roles by Source Report](#)
- [System Privileges Report and System Privileges by Source Report](#)
- [Object Privileges Report and Object Privileges by Source Report](#)
- [Privileged Users Report and Privileged Users by Source Report](#)

3.3.5.1 About the Default Entitlement Reports

An entitlement report describes the types of access that users have to an Oracle source database. It provides information about the user, role, profile, and privileges used in the source database. For example, the entitlement reports capture information such as access privileges to key data or privileges assigned to a particular user. These reports are useful for tracking unnecessary access to data, finding duplicate privileges, and simplifying privilege grants.

After you generate a default entitlement report, you can view a snapshot of the metadata that describes user, role, profile, and privilege information. This enables you to perform tasks such as comparing different snapshot labels to find how the entitlement information has changed over time. See [Section 3.8](#).

See Also:

- [Section 3.8.6](#) for information about generating and viewing entitlement report data
- [Section 3.9](#) and [Section 3.11](#) for information about creating user-defined reports from entitlement reports

3.3.5.2 User Accounts Report and User Accounts by Source Report

The User Accounts Report and User Accounts by Source Report show the following information about user accounts: source database in which the user account was created, user account name, account status (`LOCKED` or `UNLOCKED`), expiration date for the password, initial lock state (date the account will be locked), default tablespace, temporary tablespace, initial resource consumer group, when the user account was created, associated profile, and external name (the Oracle Enterprise User DN name, if one is used).

The difference between these reports is that the "by Source" report enables you to view snapshot data from a specific Oracle source database. The regular report includes snapshot label data from all Oracle source databases assigned to given labels.

3.3.5.3 User Privileges Report and User Privileges by Source Report

The User Privileges Report and User Privileges by Source Report show the following information about user privileges: source database in which the privilege was created, user name, privilege, schema owner, table name, column name, type of access (direct access or if through a role, the role name), whether the user privilege was created with the `ADMIN` option, whether the user can grant the privilege to other users, and who granted the privilege.

The difference between these reports is that the "by Source" report enables you to view snapshot data from a specific Oracle source database. The regular report includes snapshot label data from all Oracle source databases assigned to given labels.

3.3.5.4 User Profiles Report and User Profiles by Source Report

The User Profiles Report and User Profiles by Source Report show the following information about user profiles: source database in which the user profile was created, profile name, resource name, resource type (`KERNEL`, `PASSWORD`, or `INVALID`), and profile limit.

The difference between these reports is that the "by Source" report enables you to view snapshot data from a specific Oracle source database. The regular report includes snapshot label data from all Oracle source databases assigned to given labels.

3.3.5.5 Database Roles Report and Database Roles by Source Report

The Database Roles Report and Database Roles by Source Report lists names of database roles and application roles. If the role is a secure application role, then the `Schema` and `Package` columns of the report indicate the underlying PL/SQL package used to enable the role.

The difference between these reports is that the "by Source" report enables you to view snapshot data from a specific Oracle source database. The regular report includes snapshot label data from all Oracle source databases assigned to given labels.

3.3.5.6 System Privileges Report and System Privileges by Source Report

The System Privileges Report and System Privileges by Source Report show the following information about system privileges: source database in which the system privilege was created, user granted the system privilege, privilege name, type of access (direct access or if through a role, the role name), and whether it was granted with the ADMIN option.

The difference between these reports is that the "by Source" report enables you to view snapshot data from a specific Oracle source database. The regular report includes snapshot label data from all Oracle source databases assigned to given labels.

3.3.5.7 Object Privileges Report and Object Privileges by Source Report

The Object Privileges Report and Object Privileges by Source Report show the following information about object privileges: the source database in which the object was created, users granted the object privilege, schema owner, target name (which lists tables, packages, procedures, functions, sequences, and other objects), column name (that is, column-level privileges), privilege (object or system privilege, such as SELECT), type of access allowed the object (direct access or if through a role, the role name), whether the object privilege can be granted, and who the grantor was.

The difference between these reports is that the "by Source" report enables you to view snapshot data from a specific Oracle source database. The regular report includes snapshot label data from all Oracle source databases assigned to given labels.

3.3.5.8 Privileged Users Report and Privileged Users by Source Report

The Privileged Users Report and Privileged Users by Source Report show the following information about privileged users: source database in which the privileged user account was created, user name, privileges granted to the user, type of access (direct access or if through a role, the role name), and whether the privileged user was granted the ADMIN option.

The difference between these reports is that the "by Source" report enables you to view snapshot data from a specific Oracle source database. The regular report includes snapshot label data from all Oracle source databases assigned to given labels.

3.4 Using the Compliance Reports

This section contains:

- [About the Compliance Reports](#)
- [Credit Card Compliance Report: Related Data Access Compliance Report](#)
- [Financial Compliance Reports](#)
- [Health Care Compliance Report: EPHI Related Data Access Report](#)
- [Common Credit Card, Financial, and Health Care Compliance Reports](#)

See Also: [Section 3.9.4](#) for information about changing the default displayed contents of a compliance report

3.4.1 About the Compliance Reports

The compliance reports provide out-of-the-box reports to help you meet regulations associated with credit card, financial, and health care related data. They track activities that are typically required to meet standard compliance regulations, such as changes to the database structure or its objects, failed logins, administrator activities, system

events, and user logins or logoffs. Internal and external auditors request many of these reports to monitor security and compliance for your business.

The compliance reports have three categories: credit card, financial, and health care. For example, all three of the categories listed have a Database Logon Report, but each category determines the type of data shown in the report. To customize the display name, description, data output, and source database for a report, under Tasks, select the **Customize Categories** link.

To access the compliance reports, select the **Audit Reports** tab, then select **Compliance Reports**. You can create user-defined reports from the reports. See [Section 3.9](#) and [Section 3.11](#). To customize the displayed contents of the default report, see [Section 3.9.4](#).

Figure 3–3 shows the Compliance Reports page.

Figure 3–3 Compliance Reports Page



3.4.2 Credit Card Compliance Report: Related Data Access Compliance Report

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

For additional compliance reports that can be used for credit card audit data, see [Section 3.4.5](#).

3.4.3 Financial Compliance Reports

The financial compliance reports are as follows:

- [Financial Related Data Access Report](#)
- [Financial Related Data Modifications Report](#)

3.4.3.1 Financial Related Data Access Report

The Financial Related Data Access Report displays audited SQL statements that were used to access financial data, such as SELECT SQL statements.

For additional compliance reports that can be used for financial audit data, see [Section 3.4.5](#).

3.4.3.2 Financial Related Data Modifications Report

The Financial Related Data Modifications Report displays audited SQL statements that were used to modify financial data, such as Oracle Database data manipulation language (DML) activities (for example, all `INSERT`, `UPDATE`, or `DELETE` SQL statements).

For additional compliance reports that can be used for financial audit data, see [Section 3.4.5](#).

3.4.4 Health Care Compliance Report: EPHI Related Data Access Report

The EPHI (Electronic Protected Health Information) Related Data Access Report displays audited SQL statements that were used to access or modify health care data, such as Oracle Database data manipulation language (DML) activities (for example, all `INSERT`, `UPDATE`, or `DELETE` SQL statements).

For additional compliance reports that can be used for health care audit data, see [Section 3.4.5](#).

3.4.5 Common Credit Card, Financial, and Health Care Compliance Reports

The credit card, financial, and health care reports all have the following common reports:

- [Audit Setting Changes Report](#)
- [Before/After Values Report](#)
- [Database Failed Logins Report](#)
- [Database Login/Logoff Report](#)
- [Database Logoff Report](#)
- [Database Logon Report](#)
- [Database Startup/Shutdown Report](#)
- [Deleted Objects Report](#)
- [Program Changes Report](#)
- [Schema Changes Report](#)
- [System Events Report](#)
- [User Privilege Change Activity Report](#)

3.4.5.1 Audit Setting Changes Report

The Audit Settings Changes Report displays audited activity of audit setting changes (for example, changes to the `AUDIT ALL` SQL statement). It captures data such as Oracle Database Vault rules, rule sets, and factors; original content; fine grained audit policies if any were used; and proxy session IDs.

3.4.5.2 Before/After Values Report

The Before/After Values Report displays a wide range of before and after values for events such as schema owners, events, event values, timing of the event changes, and which source databases they affect. It tracks information such as the IP address and client user connections. This report is designed for users who must capture specific

before and after values of Oracle database tables using the REDO collector. Contact your Oracle Audit Vault administrator for more information about the REDO collector.

3.4.5.3 Database Failed Logins Report

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

3.4.5.4 Database Login/Logoff Report

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

3.4.5.5 Database Logoff Report

The Database Logoff Report displays information about user logoff operations, such as the user name, proxy session ID, client user information, and when the logoff operation took place.

3.4.5.6 Database Logon Report

Similar to the Database Logoff Report, the Database Logon Report shows information about user logon operations. It captures the same type of information the Database Logoff Report captures.

3.4.5.7 Database Startup/Shutdown Report

The Database Startup/Shutdown Report tracks when the source database was started and shut down, and includes information such as the user who performed the startup or shutdown operation.

3.4.5.8 Deleted Objects Report

The Deleted Objects Report displays audited SQL statements that were used to delete database objects, such as delete operations on a specific table. It tracks the user who deleted the object and the command the user used to delete the object.

3.4.5.9 Program Changes Report

The Program Changes Report displays changes to row data when an insert or update operation occurs in Oracle Database. It tracks data such as the user who performed the action the action itself, and when the action took place. This report is especially useful if you are using the redo collector to extract the before and after values of data updates.

3.4.5.10 Schema Changes Report

The Schema Changes Report displays audited data definition language (DDL) activities (for example, changes to the database schema that result from SQL ALTER, CREATE, or DROP statements). It tracks data such as the user who changed the schema, when the change took place, and the status of the change attempt.

3.4.5.11 System Events Report

The System Events Report displays audited system event activities. These audit records are generated when you audit local system processes. It tracks events such as the SQL text that caused the system event, the user responsible for it, the privilege

required for the event, and when the event took place. Examples of a local system process are starting and shutting down a database or changing database parameters.

3.4.5.12 User Privilege Change Activity Report

The User Privilege Change Activity Report displays information about the privileges that were required when users change data in the source database. It tracks data such as the SQL statements the user run, event time, and the target of the change.

3.5 Using the Critical and Warning Alert Reports

The alert reports are as follows:

- [About the Critical and Warning Alert Reports](#)
- [All Alerts Report](#)
- [Critical Alerts Report](#)
- [Warning Alerts Report](#)

See Also:

- [Section 2.12](#) for information about creating and configuring alerts
- [Section 2.13](#) for information about responding to an alert

3.5.1 About the Critical and Warning Alert Reports

The critical and warning alert reports track critical and warning alerts. An alert is raised when data in a single audit record matches a predefined alert rule condition. Alerts are grouped by associated source, by event category, and by the severity level of the alert (either warning or critical). You can create user-defined reports from these alerts; see [Section 3.9](#).

3.5.2 All Alerts Report

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

3.5.3 Critical Alerts Report

This report tracks critical alerts.

3.5.4 Warning Alerts Report

This report tracks warning alerts.

3.6 Scheduling and Creating PDF Reports

This section contains:

- [About Scheduling and Creating PDF Reports](#)
- [Scheduling and Creating a PDF Report](#)

3.6.1 About Scheduling and Creating PDF Reports

You can schedule reports to be sent to other users in PDF format. You can run the report immediately, or you can create or select a schedule to run the report at a later

time. In addition to setting a time to run the report, you can create the following components for the report:

- **A retention time for the data to be used in the report.** For example, if you schedule a report to run once a month but you only want that month's audit data in the report, then you can set a retention time to store the data for each month the report runs, and then discard the data after each month. This way, the report recipients always receives the most recent month of audit data.
- **A list of users who should be notified when the report runs.** You can notify other users of the report and either send them a notification or the report in an e-mail attachment.
- **A list of auditors who must attest to the report.** You can select one or more auditors, including yourself, to attest to the report.
- **Formatting for the report.** You can design the title to include certain components, such as the category and report names. You also can control the header and footer text for the report, as well as the orientation of the report.

3.6.2 Scheduling and Creating a PDF Report

To schedule and create a PDF report:

1. Log in to the Oracle Audit Vault Console as a user who has been granted the `AV_AUDITOR` role, as explained in [Section 1.4](#).

The Dashboard page appears.

2. Select the **Audit Reports** tab.
3. Access the Create or Schedule PDF Report page using one of the following methods:
 - Select the report from the **Default Reports, Compliance Reports, Custom Reports, or Generated Reports** secondary tab, and then click the **Create PDF** button.
 - Select the **Audit Reports** tab, and then select the **Report Schedules** secondary tab. Then click the **Create** button.

The Create or Schedule PDF Report page appears.

4. In the Create or Schedule PDF Report page, if you had selected the **Report Schedules** secondary tab, then under Create or Schedule PDF Report, first select the category and then select the name of the report from the **Category Name** and **Report Name** lists.
5. Under Schedule, select a time to run the report:
 - **Immediately** if you want to run the report right away.
 - **Specify Schedule** if you want to create a schedule to run the report. From here, select how often the report should be run, the report run time and date, and the time zone offset to reflect the time zone in which the report should appear.

- **Select Schedule** if you want to select an existing schedule for the report. From here, select the schema in the Audit Vault Server database in which the schedule is stored, and the schedule name.

A database administrator can create this schedule by using the `DBMS_SCHEDULER PL/SQL` package, assuming this user has the `EXECUTE` privilege for this package. The **Schema** list displays schemas that contain `DBMS_SCHEDULER` schedules. The **Schedule** list displays all the `DBMS_SCHEDULER` schedules in that schema. By default, **Schema** contains the `SYS` schema, which owns the `DBMS_SCHEDULER` package.

6. Under Retention, enter the retention period years and months to specify how long to keep the data in the report.

The retention period determines how long to keep the audit data in storage, based on times the report is run. For example, suppose you set the retention period to 6 months. Oracle Audit Vault will delete this audit data 6 months from the last time the report is run. If you specify the retention to be 0 years and 0 months, each night the reports clean up job deletes the PDF report. You can use this special 0 years, 0 months setting to create a PDF report for immediate viewing or printing.

7. Under Notification, select the following options, and then click **Add to List** to create a notification list:
 - For Send, select either **Notification** or **Attachment**. The **Notification** option sends the user an e-mail with a URL link to the report. The **Attachment** option attaches the PDF report to the user's e-mail.
 - From the **Template** list, select a report notification template.
 - From the **Profile** list, select a profile, which contains a list of default recipients who should receive the report.
 - If you want to send the report to additional recipients, enter their e-mail addresses in the **To e-mail** and **Cc** fields. Enter the full e-mail address. Separate multiple e-mail addresses with a comma.

8. Under Attestation, select one or more auditors who should attest to the report.

Optionally, you can set the order in which the auditors are listed in the Attestation area.

9. Under Report Formatting, specify the following:

- For Title, select one or more of the following options: **Category Name**, **Report Name**, **Generated Time**, **Filters**, **Timezone**, and **Custom**. If you select **Custom**, then enter customized text for the report title.
- For Header and Footer, select from these options: **Report Name**, **Generated Time**, **Page #**, and **Custom Text**. If you select **Custom Text**, then enter this text

in the appropriate field. You can designate these elements to appear on the left, center, or right side of the page.

- For Orientation, select either **Portrait** or **Landscape**.
10. Click the **Create PDF** button.

The PDF is stored in the database. To find and review the PDF, click the **Generated Reports** tab.

3.7 Annotating and Attesting Reports

This section contains:

- [About Annotating and Attesting Reports](#)
- [Annotating and Attesting a Report](#)

3.7.1 About Annotating and Attesting Reports

After a report has been generated, auditors can annotate and attest to the report. This enables you to create a record of all notes and attestations for the report in one place, with the most recent note and attestation listed first. If you delete the report, its associated annotation and attestations are removed as well.

3.7.2 Annotating and Attesting a Report

To annotate and attest a report:

1. Log in to the Oracle Audit Vault Console as a user who has been granted the AV_AUDITOR role, as explained in [Section 1.4](#).

The Dashboard page appears.

2. Access the list of reports to attest by using one of the following methods:
 - From the Dashboard page, select the number of the report from the Attestation Actions list.
 - Select the **Audit Reports** tab, and then select the **Generated Reports** secondary tab. Find the report that you want to annotate or attest and then click the report name. When you display the report, it appears in PDF format. Click the **Details** button to display the Details for Generated Report page.

You can quickly filter the reports if you want. See [Section 3.9.3](#) for more information.

3. In the **New Note** field, enter a note for the report.
4. Perform one of the following actions:
 - To save the note only, click the **Save** button. The note appears in the Previous Notes area.
 - To save the note and attest to the report, click the **Save & Attest** button. The note appears in the Previous Notes area and the Attestation area is updated with your user name and the time that you attested to the report.
 - To return to the report, click the **View Report** button.
5. Click **Done** when you are finished.

The Generated Reports page appears.

3.8 Generating and Comparing Snapshots of Entitlement Audit Data

This section contains:

- [About Entitlement Report Snapshots and Labels](#)
- [General Steps for Using Entitlement Reports](#)
- [Retrieving Entitlement Audit Data to Create the Snapshot](#)
- [Creating an Entitlement Snapshot Label](#)
- [Assigning Snapshots to a Label](#)
- [Viewing Entitlement Snapshot and Label Audit Data](#)

3.8.1 About Entitlement Report Snapshots and Labels

An entitlement **snapshot** captures the state of user entitlement information. The snapshot contains the metadata of users and roles that a user has to a database: system and other SQL privileges, object privileges, role privileges, and user profiles. Snapshots are created automatically whenever you retrieve the entitlement data, and only apply to Oracle Database source databases. Each snapshot is unique, and it is time-stamped in the following format:

```
MM/DD/YYYY HH:MM:SS AM/PM
```

The name for the snapshot is the time stamp assigned to it when the entitlement data was retrieved (for example, `9/22/2009 07:56:17 AM`).

Each source database can only have one snapshot of a particular time stamp. In other words, you cannot have multiple snapshots entitled `9/22/2009 07:56:17 AM` in one source database. If you retrieve entitlement audit data for all your source databases at the same time, then each source database gets its own `9/22/2009 07:56:17 AM` snapshot.

Optionally, you can group snapshots from multiple source databases by assigning these snapshots to a **label**. For example, suppose the source databases `payroll`, `sales`, and `hr` each have a `9/22/2009 07:56:17 AM` snapshot. You can create a label and then assign these three snapshots to that label. This enables you to compare the snapshot data from the three source databases at once, all in the same report.

You can filter a report to show the data from an earlier snapshot or label, or you can compare the audit data from two snapshots or two labels. This way, you can find changes that have occurred over time, from different entitlement audit data retrievals. For example, you can find how user privileges have been modified between two snapshots or labels.

The type of entitlement report determines whether you can view its audit data by snapshot or by label. The reports appended with "by Source" (for example, User Accounts by Source) provide snapshot data for specific source databases. The regular entitlement reports (such as User Accounts) enable you to view audit data across all the source databases or snapshots, based on a label.

3.8.2 General Steps for Using Entitlement Reports

The general steps that you must take to use entitlement reports are as follows:

1. Retrieve the entitlement audit data to create a snapshot.
See [Section 3.8.3](#).
2. Optionally, organize the snapshots into a group and then assign them a label.

See [Section 3.8.4](#).

3. Optionally, assign one or more snapshots to a label.

See [Section 3.8.5](#).

4. View the entitlement snapshot and label data.

See [Section 3.8.6](#). For a listing of entitlement reports, see [Section 3.3.5](#).

3.8.3 Retrieving Entitlement Audit Data to Create the Snapshot

Each time you retrieve entitlement audit data, you create a snapshot.

To retrieve the entitlement audit data:

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

[Section 1.4](#) explains how to start the Audit Vault Console. The Dashboard page appears.

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

By default, the Audit Settings page appears.

3. From the Audit Source listing, select the check boxes for the source databases that you want.

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

4. Select the **User Entitlement** option.

5. Click the **Retrieve** button.

Oracle Audit Vault displays a message letting you know that the user entitlement data is being retrieved. To check the status of the retrieval, click the **Show Status** button.

3.8.4 Creating an Entitlement Snapshot Label

If you want to organize the snapshots into a group, assign them to a label. The name LATEST is automatically assigned to the latest snapshot for each Oracle source database. Therefore, each source database has its own LATEST label for its most recent retrieval.

To create an entitlement snapshot label:

1. From the Home page, select the **Audit Reports** tab, and then select the **Entitlement Snapshots** tab.

2. Under Tasks, select **Manage Snapshot Labels**.

The Snapshot Labels page appears.

3. Click **Create**.

The Add Snapshot Label page appears.

4. Enter the following information:

- **Label Name:** Enter a name for the label. Do not name the label `LATEST`, which is a reserved word. Typically, label names are based on time, such as financial quarters. For example:

`Q1_2009`

- **Description:** Optionally, enter a brief description of the label. For example:

This label captures the snapshot 9/22/2009 07:56:17 AM data for the payroll, sales, and hr source databases.

5. Click **Save**.

The new label is listed in the Snapshot Labels page. From here, you can edit the label by selecting its name, or remove it by clicking the trash icon.

Later on, if you want to edit or remove a label, select **Manage Snapshot Labels** from the Entitlement Snapshots page. To edit the label, select the label name and then use the Edit Snapshot Label page to modify the label name and description. To remove the label, select its trash icon.

3.8.5 Assigning Snapshots to a Label

You only can assign one snapshot from each source database to a label.

To assign snapshots to a label:

1. From the Home page, select the **Audit Reports** tab, and then select the **Entitlement Snapshots** tab.
2. Select one or more source database snapshots to be assigned to a label.
3. Click the **Assign Label** button.

The Assign Label page appears. The following example shows two snapshots listed for a source database called `avsource`.

The screenshot shows the 'Assign Label' interface. At the top, there are 'Cancel' and 'Save' buttons. Below them is a dropdown menu for 'Label' currently set to 'New Label -'. Underneath is a large text area for 'Description'. At the bottom, there is a 'Snapshots' section with a list containing one entry: 'avsource 9/22/2009 07:56:17 AM'.

4. Enter the following information:
 - **Label:** For a new label, enter the name in the **Label** field. To select an existing label, select the label name from the **Label** list.
 - **Description:** For a new label, optionally enter a brief description of the label.
 - **Snapshots:** Ensure that the snapshots listed are the correct snapshots. If they are incorrect, then click **Cancel** and then select the correct snapshots.
5. Click **Save**.

The label assignment appears in the Entitlement Snapshots page. From here, you can modify or move the label assignments for the snapshots.

3.8.6 Viewing Entitlement Snapshot and Label Audit Data

This section contains:

- [About Viewing Entitlement Snapshot and Label Audit Data](#)
- [Checking Entitlement Reports for Individual Snapshot or Label Audit Data](#)
- [Checking Entitlement Reports for Changes to Snapshot or Label Audit Data](#)

3.8.6.1 About Viewing Entitlement Snapshot and Label Audit Data

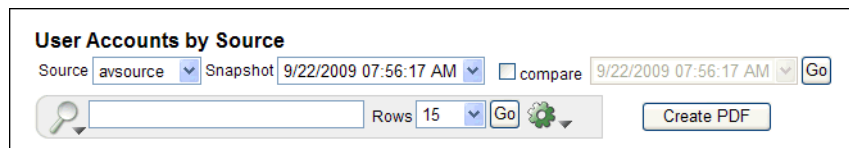
After snapshots have been created and if you have created and assigned labels for them, then you are ready to check the entitlement reports.

3.8.6.2 Checking Entitlement Reports for Individual Snapshot or Label Audit Data

To check entitlement reports for individual snapshot or label audit data:

1. Log in to the Audit Vault Console as a user who has been granted the AV_AUDITOR role.
[Section 1.4](#) explains how to start the Audit Vault Console. The Dashboard page appears.
2. Select the **Audit Reports** tab, and in the Default Reports page, under Entitlement Reports, select link for the entitlement report that you want.
3. In the entitlement report, do the following:
 - For a "by Source" report, from the **Source** list, select the source database for the snapshot that you want.
 - From the **Snapshot** or **Label** list, select the snapshot or label.

For example:



4. Click the **Go** button that is to the right of the **compare** list.

The entitlement report data appears. The generated report contains an additional column, either **Snapshot** or **Label**, indicating which snapshot or label was used for the report. From here, you can expand the **Snapshot** or **Label** column to filter its contents.

[Figure 3-4](#) shows how the User Accounts by Source Report typically appears with generated snapshot audit data.

Figure 3–4 Showing Individual Snapshot or Label Audit Data

Source	Snapshot	User	Account Status	Expiration Date	Initial Lock Date	Default Tablespace	Temporary Tablespace
avsource	9/22/2009 07:56:17 AM		EXPIRED	9/21/2009 07:57:50 PM		SYSAUX	
avsource	9/22/2009 08:2:58 AM		OPEN			SYSAUX	

3.8.6.3 Checking Entitlement Reports for Changes to Snapshot or Label Audit Data

To compare the audit data for two snapshots or labels:

1. Log in to the Audit Vault Console as a user who has been granted the AV_AUDITOR role.
Section 1.4 explains how to start the Audit Vault Console. The Dashboard page appears.
2. Select the **Audit Reports** tab, and in the Default Reports page, under Entitlement Reports, select the link for the entitlement report that you want.
3. In the report, do the following:
 - For a "by Source" report, from the **Source** list, select the source database for the snapshot that you want.
 - From the **Snapshot** or **Label** list, select the first snapshot or label.
 - Click the **compare** check box.
 - Select from the second snapshot or label list.

For example:

4. Click the **Go** button that is to the right of the **compare** list.

The entitlement report data appears. It contains an additional column entitled **Change Category**, and **- Changes** is appended to the name of the report. The Change Category column shows how the data has changed between the two snapshots or labels. From here, you can filter the data to show only **MODIFIED**, **NEW**, **DELETED**, or **UNCHANGED** data.

Figure 3–5 shows how the User Accounts - Changes Report typically appears with generated comparison data. No deletions have occurred in this label; otherwise, the **Change Category** column would include a **DELETED** category.

Figure 3–5 Comparing Entitlement Report Snapshot or Label Audit Data

Source	Label	Change Category	User	Account Status	Expiry Date	Lock Date
avsource	Q1_2009			KPIRED	9/21/2009 07:57:50 PM	
avsource	Q2_2009	MODIFIED		KPIRED	9/21/2009 07:57:50 PM	
avsource	Q1_2009	UNCHANGED	APEX_030200	OPEN		

3.9 Controlling the Display of Data in a Report

This section contains:

- [About Controlling the Display of Report Data](#)
- [Hiding or Showing Columns in a Report](#)
- [Filtering Data in a Report](#)
- [Changing the Default Displayed Contents of a Compliance Report](#)
- [Sorting Data in a Report](#)
- [Highlighting Rows in a Report](#)
- [Charting Data in a Report](#)
- [Adding a Control Break to a Column in a Report](#)
- [Resetting the Report Display Values to Their Default Settings](#)

See Also: [Section 3.8.6](#), which describes additional ways that you can view audit data in entitlement reports

3.9.1 About Controlling the Display of Report Data

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

3.9.2 Hiding or Showing Columns in a Report

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

This section contains:

- [Hiding the Currently Selected Column](#)
- [Hiding or Showing Any Column](#)

3.9.2.1 Hiding the Currently Selected Column

To hide the currently selected column:

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

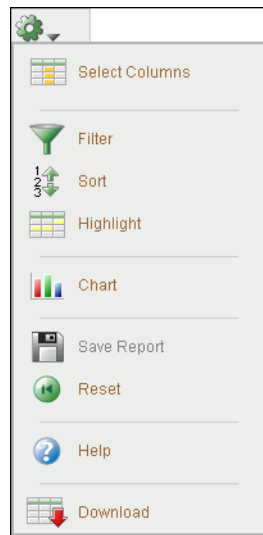
- In the **Column Heading** menu, click the **Hide Column** button.

3.9.2.2 Hiding or Showing Any Column

To hide or show columns in a report:

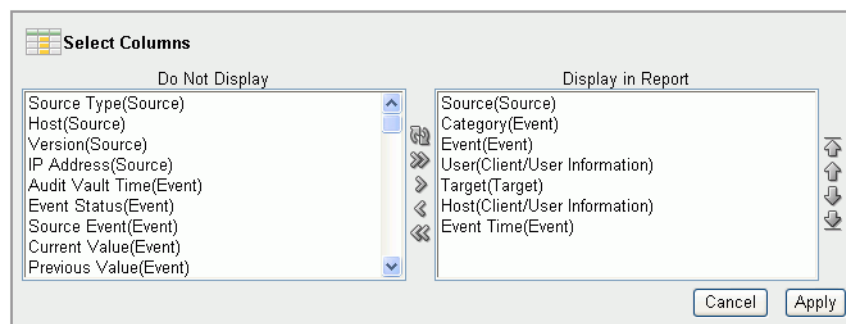
- Access the report that you want.
[Section 3.2](#) explains how to access a report.
- Select the **Actions** menu (gear) icon on the Search bar.

The Actions menu appears.



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

The Select Columns dialog field appears under the Search bar.



- To move column names between the **Do Not Display** and **Display in Report** boxes:
 - Select the column names to move and then click the left or right arrow between the column name boxes.
 - Move all columns left or right by using the >> and << buttons.
 - Use the top button (the arrows in a circle) to reset the columns to their original locations in the two boxes.
- To set the order of appearance in the report for displayed columns, in the **Display in Report** box, select the column name, then click the up arrow or down arrow on the right side of the box to reorder its position in the list.

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

6. Click **Apply**.

3.9.3 Filtering Data in a Report

This section contains:

- [About Filtering Data in Reports](#)
- [Filtering All Rows Based on Data from the Currently Selected Column](#)
- [Filtering Column and Row Data](#)
- [Filtering Row Data Using an Expression](#)

3.9.3.1 About Filtering Data in Reports

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

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

See Also: [Section 3.9.4](#) for information about using filters to change the default definition of the contents of a compliance report

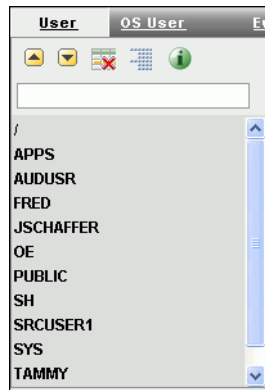
3.9.3.2 Filtering All Rows Based on Data from the Currently Selected Column

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

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

1. Access the report that you want.
[Section 3.2](#) explains how to access a report.
2. Under the report name, select the column that you want to use as a basis for the filter.

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



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

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

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

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

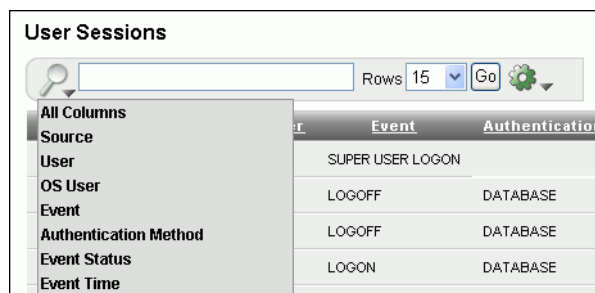
3.9.3.3 Filtering Column and Row Data

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

To search for row data in one or all columns:

1. Access the report that you want.
[Section 3.2](#) explains how to access a report.
2. If you want to focus the search on a specific column, in the Search bar, use the Search icon to select from the list of available columns.

By default, Oracle Audit Vault searches all columns.



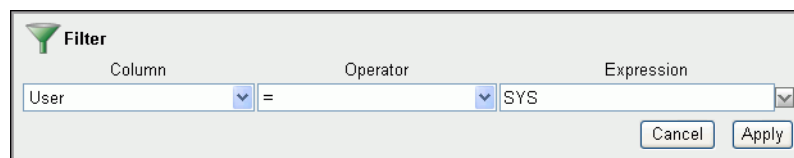
3. In the Search bar text area, enter all or part of the text in the column row that you want.
 For example, enter `SYS` to find all user names that contain the letters `SYS`.
 The search is not case-sensitive.
4. In the **Rows** list, select the number of rows that you want to appear on each page.
 The default is 15 rows.
5. Click **Go**.

3.9.3.4 Filtering Row Data Using an Expression

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

To filter row data using an expression:

1. Access the report that you want.
[Section 3.2](#) explains how to access a report.
2. Select the **Actions** menu (gear) icon on the Search bar.
3. Select **Filter**.
 The Filter dialog box appears under the Search bar.
4. Enter the following information:
 - **Column:** Select the name of the column from the list. Note that you can select all columns, including hidden columns.
 - **Operator:** Select a SQL operator from the list, for example, `>` for "greater than" or `=` for "equals."
 - **Expression:** Select an expression from the list. The expression lists the row data (for example, names of users found in the `User` column). If you type the expression in the **Expression** field, remember that the expression is case-sensitive. In most cases, use uppercase letters.



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

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

3.9.4 Changing the Default Displayed Contents of a Compliance Report

Each compliance report has a hidden filter that controls the displayed contents of the default version of the report. You can display and then modify the definition of this filter if you want to customize the compliance report data. Alternatively, you can remove this filter and create new filters for further customization.

To change the definition of the default displayed contents of a compliance report:

1. Access the compliance report that you want.
[Section 3.2](#) explains how to access a report.
2. Click the **Change Definition** button.

Source	Owner	Target	User	OS User	Event Status	Host	Event Time
oracle1	SH	SALES	SH	MALOEUF	UNKNOWN:FGA	binks241	11/9/2009 11:17:34 AM
oracle1	OE	ORDERS	OE	MALOEUF	UNKNOWN:FGA	binks241	11/9/2009 11:17:34 AM

The report window changes to display the default, hidden filter for the compliance report. For example, for the Credit Card Related Data Access Report, this filter is ListOfCreditCardObjects.

Source	Owner	Target	User	OS User	Event Status	Host	Event Time
oracle1	SH	SALES	SH	MALOEUF	UNKNOWN:FGA	binks241	11/9/2009 11:17:34 AM
oracle1	OE	ORDERS	OE	MALOEUF	UNKNOWN:FGA	binks241	11/9/2009 11:17:34 AM

3. Select the link for the hidden filter.
For the Credit Card Related Data Access Report, you would select the **Target contains 'ListOfCreditCardObjects'** link. Afterwards, the Filter region appears.
4. In the Filter region, modify the default filter definition.
See [Section 3.9.3](#) for detailed information about filtering data in a report.
5. Click the **Save Definition** button.

3.9.5 Sorting Data in a Report

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

This section contains:

- [Sorting Row Data for the Currently Selected Column](#)
- [Sorting Row Data for All Columns](#)

3.9.5.1 Sorting Row Data for the Currently Selected Column

To sort row data for the current column:

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

3.9.5.2 Sorting Row Data for All Columns

To sort row data for all columns:

1. Access the report that you want.
[Section 3.2](#) explains how to access a report.
2. Select the **Actions** menu (gear) icon on the Search bar.
3. In the Actions Menu, select **Sort**.

The Sort dialog box appears under the Search bar.

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

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

3.9.6 Highlighting Rows in a Report

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

To highlight rows in the report:

1. Access the report that you want.
[Section 3.2](#) explains how to access a report.
2. Select the **Actions** menu (gear) icon on the Search bar.
3. In the Actions menu, select **Highlight**.
The Highlight dialog box appears under the Search bar.
4. Enter the following information:
 - **Name:** Enter a name for this highlight instance. (Optional)

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

The screenshot shows the 'Highlight' dialog box with the following configuration:

- Name:** SYS users accessing payroll DB
- Sequence:** 10
- Enabled:** Yes
- Highlight Type:** Row
- Background Color:** #FFFFCC
- Text Color:** #3366CC
- Highlight Condition:**
 - Column:** User
 - Operator:** =
 - Expression:** SYS

5. Click **Apply**.

3.9.7 Charting Data in a Report

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

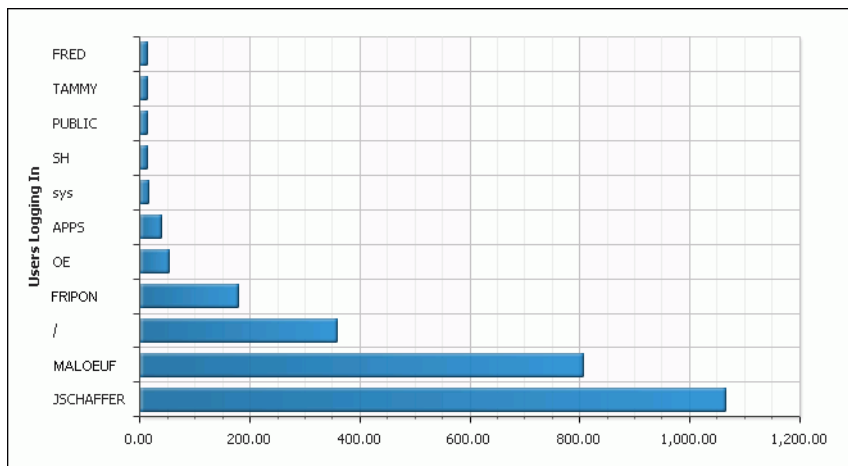
To chart data in a report:

1. Access the report that you want.
[Section 3.2](#) explains how to access a report.
2. Select the **Actions** menu (gear) icon on the Search bar, and then select **Chart**.
 The Chart dialog box appears under the Search bar.
3. Enter the following information:

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

4. Click **Apply**.

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



3.9.8 Adding a Control Break to a Column in a Report

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

To add a control break in a column:

1. Access the report that you want.

[Section 3.2](#) explains how to access a report.

2. Select the column to which you want to add a control break.
3. In the Column Heading menu, select the **Control Break** icon.

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

3.9.9 Resetting the Report Display Values to Their Default Settings

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

To reset the display settings to their defaults:

1. Access the report that you want.

[Section 3.2](#) explains how to access a report.

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

3.10 Finding Information About Report Data

This section contains:

- [Finding Detailed Information About an Audit Record](#)
- [Finding Information About the Purpose of a Column](#)

3.10.1 Finding Detailed Information About an Audit Record

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


To find detailed information about an audit record:

1. Access the report that you want.

[Section 3.2](#) explains how to access a report.

2. Use the methods described in [Section 3.9](#) to find the audit record.
3. Select the Audit Record Details icon, which appears to the left of the first column in the report.

A detailed report for the audit record appears.

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

3.10.2 Finding Information About the Purpose of a Column

To find information about the purpose of a column:

1. Access the report that you want.

[Section 3.2](#) explains how to access a report.

2. Select the column on which you want information.

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

3.11 Working with User-Defined Reports

This section contains:

- [About User-Defined Reports](#)
- [Creating a Category for User-Defined Reports](#)
- [Creating a User-Defined Report](#)
- [Accessing a User-Defined Report](#)

3.11.1 About User-Defined Reports

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

3.11.2 Creating a Category for User-Defined Reports

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

This section contains:

- [Creating a Category Name](#)
- [Alphabetizing the Category Name List](#)
- [Editing a Category Name](#)

3.11.2.1 Creating a Category Name

To create a category name for user-defined reports:

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

3.11.2.2 Alphabetizing the Category Name List

To alphabetize the category name list:

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

3.11.2.3 Editing a Category Name

To edit a category name:

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

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

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

3.11.3 Creating a User-Defined Report

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

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

To create a user-defined report:

1. Access the report that you want.
 - [Section 3.2](#) explains how to access a report.
2. Use the methods described in [Section 3.9](#) to design the display of data as needed.
3. Select the **Actions** menu (gear) icon on the Search bar, and then select **Save Report**. The Save Report dialog box appears, under the Search bar.
4. Enter the following information:
 - **Name:** Enter a name for the report.
 - **Category:** Select from the list of available categories. If you select **New Category**, then enter a name for the new category.
 - If you must create a new category, see [Section 3.11.2](#).
 - **Description:** Enter a brief description of the report.
 - **Public:** Select this check box to enable the report to be accessible to all Oracle Audit Vault users.
5. Click **Apply**.

3.11.4 Accessing a User-Defined Report

To access a user-defined report:

1. Log in to the Oracle Audit Vault Console as a user who has been granted the AV_AUDITOR role, as explained in [Section 1.4](#).
 - The Dashboard page appears.
2. Select the **Audit Reports** tab, and then select the **Custom Reports** secondary tab.
3. In the **Report Name** column, select the link for the report that you want to access.
 - The report appears. Its report details icon and filter definitions appear after the Search bar. From here, you can click the **Saved Report** link to change the report settings, delete the report, or disable and enable the report filters.



3.12 Downloading a Report to a CSV File

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

To download a report to a CSV file:

1. Access the report that you want.
[Section 3.2](#) explains how to access a report.
2. Select the **Actions** menu (gear) icon on the Search bar, and then select.
3. In the Download dialog box, select **CSV**.
4. In the File Download dialog box, enter a name for the file.
5. Click **Save** to save the file to a location in your file system.

Oracle Audit Vault Data Warehouse Schema

This chapter contains:

- [About the Oracle Audit Vault Data Warehouse Schema](#)
- [Oracle Audit Vault Audit Data Warehouse Architecture](#)
- [Design of the Audit Data Warehouse Schema](#)
- [How the Fact Table and Dimension Tables Work](#)
- [Fact Table Constraints and Indexes](#)
- [Relationships Between the Fact and Dimension Tables](#)
- [Accessing Data Trace Values](#)

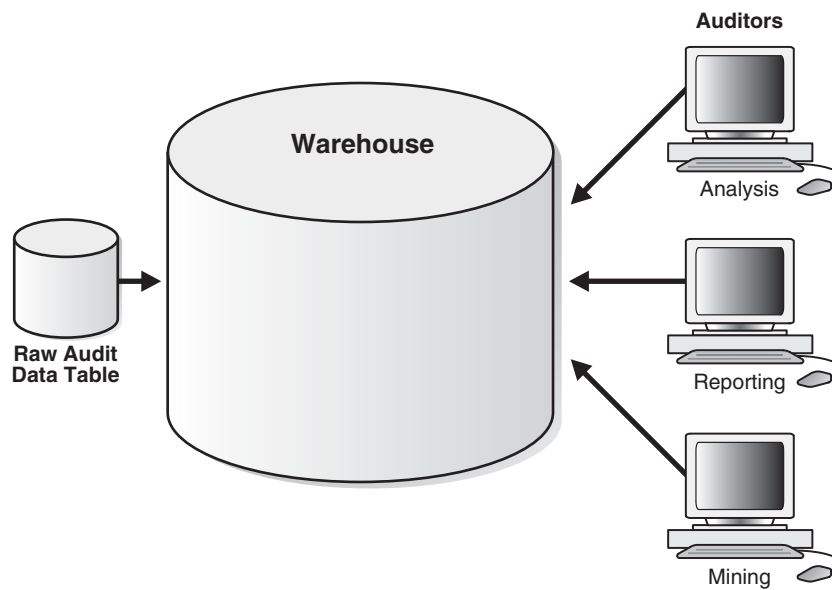
4.1 About the Oracle Audit Vault Data Warehouse Schema

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

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

4.2 Oracle Audit Vault Audit Data Warehouse Architecture

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

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

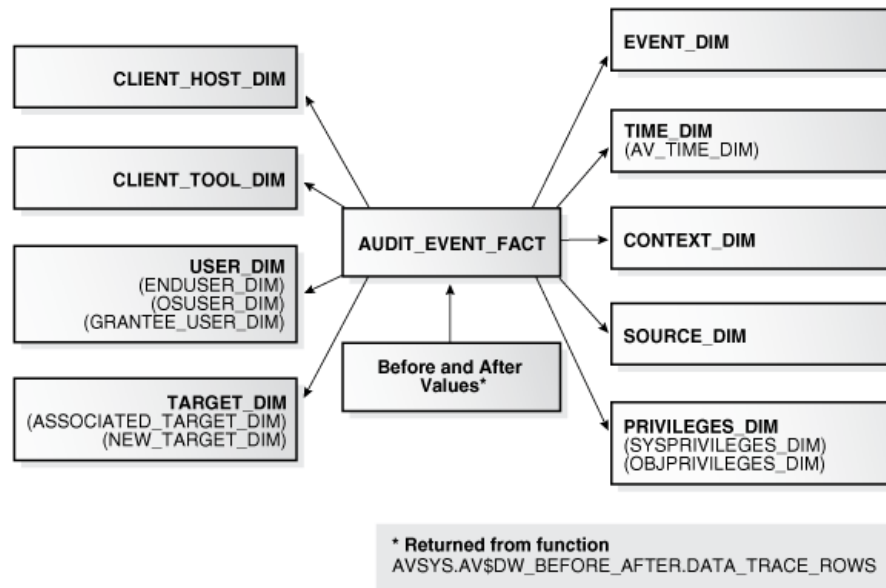
Audit records, stored in the raw audit data table go through an extraction and transformation process before the data loading process (ETL). The ETL operation takes place in the staging area. Oracle Audit Vault optimizes data in the data warehouse for data analysis, and includes the metadata and summaries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

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

4.3 Design of the Audit Data Warehouse Schema

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

Figure 4–2 shows how Oracle Audit Vault uses a star schema to model 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. For this star schema, the audit record is an entity (the fact table, `AUDIT_EVENT_FACT`) in the center of the star. The surrounding dimension tables describe the attributes of the `AUDIT_EVENT_FACT` fact table. If the audit records in the `AUDIT_EVENT_FACT` table have before and after values, then they can be accessed using the procedure described in "Accessing Data Trace Values" on page 4-18.

Figure 4–2 Structure of the Oracle Audit Data Warehouse

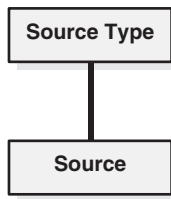
The audit data warehouse involves a fact (the entity), which is an action, and dimensions (the attributes), which are details about the action. For example, a login attempt is a fact (an audit record). Who logged on, onto what system, at what time, using what authentication system, using what user name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

4.4 How the Fact Table and Dimension Tables Work

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

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

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

Figure 4–3 Source Dimension Hierarchy

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

The audit data warehouse includes the following dimensions:

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

The `TARGET_DIM` dimension table, described in [Section 4.6.8](#), stores this information. Oracle Audit Vault updates the `TARGET_DIM` table dynamically as audit records are entered into the raw audit data table. The target name is stored with the owner name appended to the target name (for example, `SCOTT.EMP` to represent the `EMP` table in the `SCOTT` schema).

- **Event.** This dimension is built on the various events that can be performed in any of the source databases. Oracle Audit Vault uses a category of events to group events, and this forms the hierarchy used by this dimension. The `EVENT_DIM` dimension table, described in [Section 4.6.5](#), stores this information.
- **Time.** This dimension tracks actions over time. It is the most common use of the Oracle Audit Vault data warehouse. The hierarchy for time is based on calendar year.

The `TIME_DIM` dimension table, described in [Section 4.6.9](#), stores this information. The time dimension tracks event time as well as for the time when the record was received into the raw audit data table. The granularity of the time dimension is one day, and the actual time of the event and recording of the event are stored as measures in the fact table. Oracle Audit Vault uses this time measurement to filter events to granularity smaller than a day.

- **Context.** This dimension is used to represent the context information related to the audit event. This dimension has three levels: `sub_context`, `context`, and `parent_context`. You can use these levels to group events based on the context during

analysis. The CONTEXT_DIM dimension table, described in [Section 4.6.4](#), stores this information.

- **Source.** This dimension consists of the list of source databases that send audit data to the data warehouse. The SOURCE_DIM dimension table, described in [Section 4.6.7](#), stores this information.
- **Privileges.** This dimension represents the information about the privileges used during the event. There is no hierarchy for this dimension. The PRIVILEGES_DIM dimension table, described in [Section 4.6.6](#), stores this information.

4.5 Fact Table Constraints and Indexes

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

Table 4–1 Fact Table Constraints and Indexes

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

[Table 4–2](#) lists the local bitmap indexes in the AUDIT_EVENT_FACT table.

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

Index Name	Column Name
CLIENT_HOST_DIM_IDX	CLIENT_HOST_DIM
EVENT_DIM_IDX	EVENT_DIM
OSUSER_DIM_IDX	OSUSER_DIM
TARGET_DIM_IDX	TARGET_DIM

Table 4–2 (Cont.) Local Bitmap Indexes Defined on the AUDIT_EVENT_FACT Table

Index Name	Column Name
USER_DIM_IDX	USER_DIM

4.6 Relationships Between the Fact and Dimension Tables

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

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

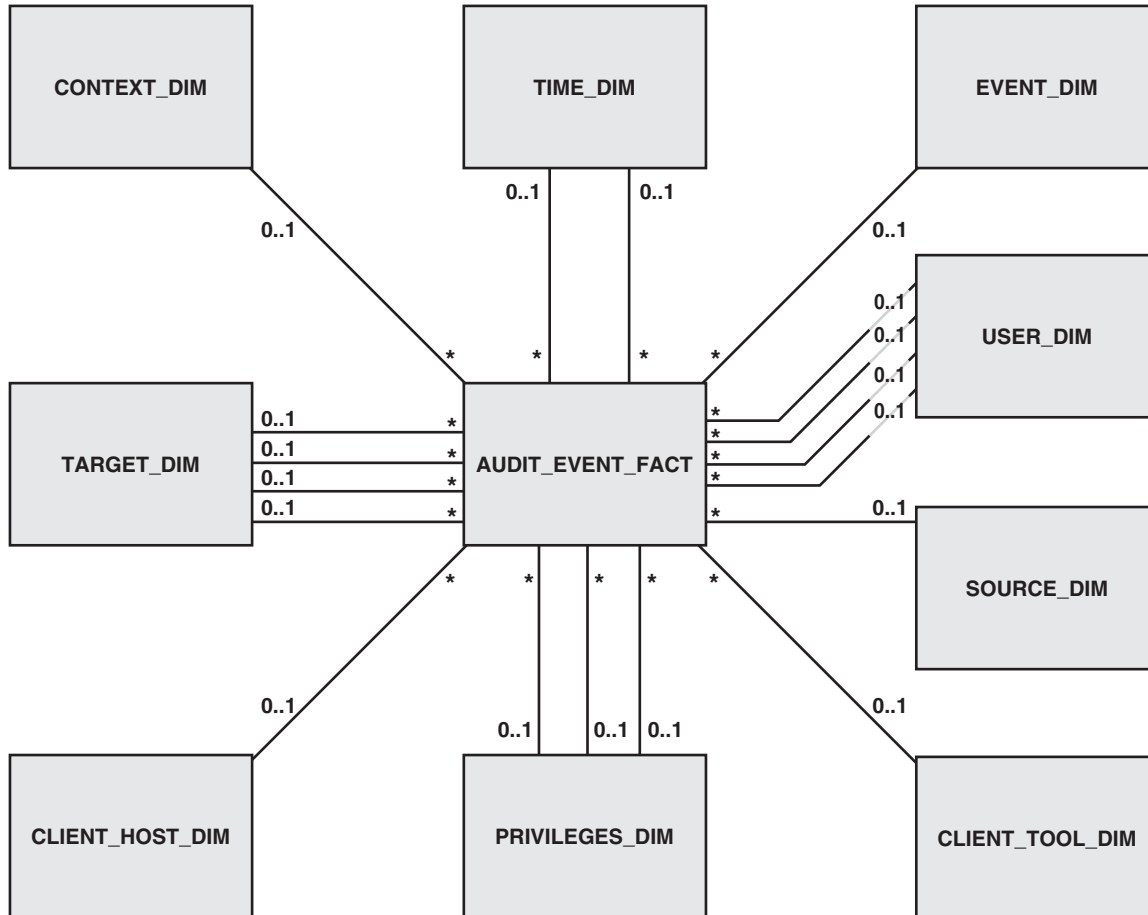


Table 4–3 through Table 4–12 contain information about the individual tables, including their columns, the data types for those columns, and whether the columns are allowed to be null. When the column is actually a reference to a dimension table, the referenced table is also listed. The asterisk and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

4.6.1 AUDIT_EVENT_FACT Fact Table

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

Table 4–3 AUDIT_EVENT_FACT Fact Table

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

Table 4–3 (Cont.) AUDIT_EVENT_FACT Fact Table

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

Table 4–3 (Cont.) AUDIT_EVENT_FACT Fact Table

Column	Data Type	References	Description
ERROR_MESSAGE_STR	VARCHAR2(4000)	None	Error message text
EVENT_DIM	NUMBER	EVENT_DIM	Dimension key to the EVENT_DIM table, which contains information about various events that can be performed in the source databases
EVENT_STATUS_ID	NUMBER	None	ID of the EVENT_STATUS_TAB table, which contains the status of the audit action. If the action was successful, it shows a status of 0 - Action. If the action was unsuccessful, it shows the error code that the action generates, such as 2004 - Security violation for an Oracle Database security violation.
EVENT_SUB_CLASS_NUM	NUMBER	None	Type of event subclass. This data column is not populated for all event classes.
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE	None	Date and time of the creation of the audit trail entry (date and time of the user login for entries created by AUDIT SESSION) in the local database session time zone
FACTOR_CONTEXT_STR	VARCHAR2(4000)	None	The Oracle Database Vault factor identifiers for the current session at the point when the audit event was triggered
FGA_POLICYNAME_ID	NUMBER	None	Fine-grained audit policy name; only applies to Oracle Database
GRANTEE_USER_DIM	NUMBER	USER_DIM	Dimension key to the USER_DIM table, which tracks information about the user who is associated with the events that occur in the source database
GUID_NUM	NUMBER	None	Global user identifier value, which is dependent on the event class captured in the trace
INDEX_ID_NUM	NUMBER	None	Index ID associated with an audit event
INSTANCE_NUMBER_NUM	NUMBER	None	The database instance number in an Oracle Real Applications Cluster
IS_SYSTEM_NUM	NUMBER	None	Indicates whether the event occurred on a system process or a user process: <ul style="list-style-type: none"> ■ 1: system ■ 0: user

Table 4–3 (Cont.) AUDIT_EVENT_FACT Fact Table

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

Table 4–3 (Cont.) AUDIT_EVENT_FACT Fact Table

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

Table 4–3 (Cont.) AUDIT_EVENT_FACT Fact Table

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

4.6.2 CLIENT_HOST_DIM Dimension Table

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

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

Table 4-4 CLIENT_HOST_DIM Dimension Table

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

4.6.3 CLIENT_TOOL_DIM Dimension Table

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

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

Table 4-5 CLIENT_TOOL_DIM Dimension Table

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

4.6.4 CONTEXT_DIM Dimension Table

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

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

Table 4-6 CONTEXT_DIM Dimension Table

Column	Data Type	Description
CONTEXT	VARCHAR2 (4000)	Session ID of the audit event
CONTEXT_ID	NUMBER	An internal cross-reference to the CONTEXT column.
DIMENSION_KEY	NUMBER	Dimension key to the AUDIT_EVENT_FACT fact table
PARENT_CONTEXT	VARCHAR2 (4000)	Sequence number or identifier of a transaction

Table 4–6 (Cont.) CONTEXT_DIM Dimension Table

Column	Data Type	Description
PARENT_CONTEXT_ID	NUMBER	Sequence number or identifier of a transaction
SUB_CONTEXT	VARCHAR2 (4000)	Transaction ID
SUB_CONTEXT_ID	NUMBER	An internal cross-reference to the SUB_CONTEXT column

4.6.5 EVENT_DIM Dimension Table

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

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

Table 4–7 EVENT_DIM Dimension Table

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

4.6.6 PRIVILEGES_DIM Dimension Table

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

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

Table 4–8 PRIVILEGES_DIM Dimension Table

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

4.6.7 SOURCE_DIM Dimension Table

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

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

Table 4–9 SOURCE_DIM Dimension Table

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

4.6.8 TARGET_DIM Dimension Table

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

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

Table 4–10 TARGET_DIM Dimension Table

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

Table 4–10 (Cont.) TARGET_DIM Dimension Table

Column	Data Type	Description
TARGET_ID	NUMBER	ID of the target object that is being audited
TARGET_NAME	VARCHAR2 (4000)	Name of the target object that is being audited

4.6.9 TIME_DIM Dimension Table

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

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

Table 4–11 TIME_DIM Dimension Table

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

Table 4–11 (Cont.) TIME_DIM Dimension Table

Column	Data Type	Description
CALENDAR_QUART_OF_YEAR	NUMBER	Numeric representation of the calendar quarter (for example, 2 for the second quarter of the year)
CALENDAR_QUART_START_DATE	DATE	Start date of the MONTH level (for example, 1-feb-08)
CALENDAR_QUART_TIME_SPAN	NUMBER	Duration of the QUARTER level (for example, 90)
CALENDAR_YEAR_CODE	NUMBER	Numeric representation for the YEAR level (for example, 2008 for the year 2008)
CALENDAR_YEAR_DESCRIPTION	VARCHAR2 (255)	Text description for the YEAR level (for example, 2008)
CALENDAR_YEAR_END_DATE	DATE	End date for the YEAR level (for example, 31-dec-08)
CALENDAR_YEAR_ID	NUMBER	ID of the YEAR level
CALENDAR_YEAR_NAME	VARCHAR2 (255)	Same as CALENDAR_YEAR_DESCRIPTION
CALENDAR_YEAR_START_DATE	DATE	Start date of the YEAR level (for example, 1-jan-08)
CALENDAR_YEAR_TIME_SPAN	NUMBER	Duration of the YEAR level (for example, 360)
DAY	DATE	Numeric representation of the day (for example, 14 for the 14th day)
DAY_CODE	NUMBER	Numeric representation for the DAY level (for example, 20080214 for February 12, 2008)
DAY_DESCRIPTION	VARCHAR2 (255)	Text description of for the DAY level (for example, 14 for the 14th day of the month)
DAY_END_DATE	DATE	End date for the DAY level (for example, 29-feb-08)
DAY_ID	NUMBER	ID for the DAY level
DAY_NAME	VARCHAR2 (255)	Same as DAY_DESCRIPTION
DAY_OF_CAL_MONTH	NUMBER	Numeric representation of the day of the calendar month (for example, 14)
DAY_OF_CAL_QUARTER	NUMBER	Numeric representation of the day of the calendar quarter (for example, 14)
DAY_OF_CAL_WEEK	NUMBER	Numeric representation of the day of the calendar week (for example, 7)
DAY_OF_CAL_YEAR	NUMBER	Numeric representation of the day of the calendar year (for example, 14)
DAY_START_DATE	DATE	Start date of the DAY level (for example, 1-feb-08)

Table 4–11 (Cont.) TIME_DIM Dimension Table

Column	Data Type	Description
DAY_TIME_SPAN	NUMBER	Duration of the DAY level (for example, 1)
DIMENSION_KEY	NUMBER	Unique key across all levels

4.6.10 USER_DIM Dimension Table

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

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

Table 4–12 USER_DIM Dimension Table

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

4.7 Accessing Data Trace Values

You can include before and after values that have been collected from the Oracle redo logs in your data warehouse queries. To do so, use the `AVSYS.AV$DW_BEFORE_AFTER` PL/SQL package. Only users who have been granted the `AV_AUDITOR` role can invoke this package. This package contains one function, `DATA_TRACE_ROWS`, which is a pipelined table function that can create a virtual table listing before and after values from the redo log.

The syntax for the `DATA_TRACE_ROWS` function is as follows:

```
AV$DW_BEFORE_AFTER.DATA_TRACE_ROWS (
  rec_id   IN NUMBER,
  src_dim  IN NUMBER,
  rec_time IN TIMESTAMP WITH LOCAL TIME ZONE)
RETURN before_after_tab PIPELINED;
```

In this specification:

- `rec_id` refers to the record ID number from in the `RECORD_ID` column in the `AUDIT_EVENT_FACT` table.
- `src_dim` refers to the source dimension table number from the `SOURCE_DIM` column in the `AUDIT_EVENT_FACT` table.
- `rec_time` refers to the time that the record was created in the Audit Vault repository, based on the local time zone. It comes from the `AV_TIME` column in the `AUDIT_EVENT_FACT` table.

Example 4–1 shows a query that uses the `DATA_TRACE_ROWS` function to include before and after values in a report similar to the Data Access Report you can access through the user interface."

Example 4–1 Using the DATA_TRACE_ROWS Function to Access Data Trace Values

```
select t.owner_name||'.'||t.target_name table_name, e.event_name,
       f.event_time, x.column_name, x.old_value, x.new_value
from event_dim e, target_dim t, audit_event_fact f,
table(av$dw_before_after.data_trace_rows(f.record_id, f.source_dim,
f.av_time)) x
where f.event_dim = e.dimension_key
and f.target_dim = t.dimension_key
and f.data_values_cnt > 0;
```

See Also: [Section 3.3.2.3](#) for information about the Data Access Report

Oracle Database Audit Events

This appendix contains:

- [About the Oracle Database Audit Events](#)
- [Account Management Events](#)
- [Application Management Events](#)
- [Audit Command Events](#)
- [Data Access Events](#)
- [Oracle Database Vault Events](#)
- [Exception Events](#)
- [Invalid Record Events](#)
- [Object Management Events](#)
- [Peer Association Events](#)
- [Role and Privilege Management Events](#)
- [Service and Application Utilization Events](#)
- [System Management Events](#)
- [Unknown or Uncategorized Events](#)
- [User Session Events](#)

A.1 About the Oracle Database Audit Events

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

- **For alerts.** When you create an alert, you can specify an audit event, based on its category, that can trigger the alert. See [Section 2.12.4](#) for more information.
- **For custom reports using third-party tools.** If you want to create custom reports using other Oracle Database reporting products or third-party tools, then refer to the tables in this appendix when you design the reports. See [Chapter 4, "Oracle Audit Vault Data Warehouse Schema"](#) for more information about custom reports created with third-party tools.

A.2 Account Management Events

Account management events track SQL statements that affect user accounts, such as creating users or altering their profiles. The Account Management Report, described in [Section 3.3.3.2](#), uses these events.

[Table A-1](#) lists the Oracle Database account management source database events and the equivalent Oracle Audit Vault events.

Table A-1 Oracle Database Account Management Audit Events

Event Name Description	Source Event	Audit Vault Event
ALTER PROFILE	67	ALTER PROFILE
ALTER USER	43	ALTER USER
CREATE PROFILE	65	CREATE PROFILE
CREATE USER	51	CREATE USER
DROP PROFILE	66	DROP PROFILE
DROP USER	53	DROP USER

[Table A-2](#) lists the Oracle Database account management event attributes.

Table A-2 Oracle Database Account Management Event Attributes

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

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

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

¹ SQL_BIND variable could be truncated to 4000 characters.

² SQL_TEXT variable could be truncated to 4000 characters.

A.3 Application Management Events

Application management events track actions that were performed on the underlying PL/SQL procedures or functions of system services and applications, such as ALTER FUNCTION statements. The Procedure Management Report, described in [Section 3.3.3.5](#), uses these events.

[Table A–3](#) lists the Oracle Database application management source database events and the equivalent Oracle Audit Vault events.

Table A–3 Oracle Database Application Management Audit Events

Event Name Description	Source Event	Audit Vault Event
ALTER ASSEMBLY (Release 11.2)	217	ALTER ASSEMBLY
ALTER FUNCTION	92	ALTER FUNCTION
ALTER JAVA	161	ALTER JAVA
ALTER PACKAGE	95	ALTER PACKAGE
ALTER PACKAGE BODY	98	ALTER PACKAGE BODY
ALTER PROCEDURE	25	ALTER PROCEDURE
ALTER RESOURCE COST	70	ALTER RESOURCE COST
ALTER REWRITE EQUIVALENCE	210	ALTER REWRITE EQUIVALENCE
ALTER TRIGGER	60	ALTER TRIGGER
ALTER TYPE	80	ALTER TYPE
ALTER TYPE BODY	82	ALTER TYPE BODY
ANALYZE INDEX	63	ANALYZE INDEX
ANALYZE TABLE	62	ANALYZE TABLE
ASSOCIATE STATISTICS	168	ASSOCIATE STATISTICS
CREATE ASSEMBLY (Release 11.2)	216	CREATE ASSEMBLY

Table A-3 (Cont.) Oracle Database Application Management Audit Events

Event Name Description	Source Event	Audit Vault Event
CREATE CONTEXT	177	CREATE CONTEXT
CREATE FUNCTION	91	CREATE FUNCTION
CREATE INDEXTYPE	164	CREATE INDEXTYPE
CREATE JAVA	160	CREATE JAVA
CREATE LIBRARY	159	CREATE LIBRARY
CREATE OPERATOR	163	CREATE OPERATOR
CREATE PACKAGE	94	CREATE PACKAGE
CREATE PACKAGE BODY	97	CREATE PACKAGE BODY
CREATE PROCEDURE	24	CREATE PROCEDURE
CREATE TRIGGER	59	CREATE TRIGGER
CREATE TYPE	77	CREATE TYPE
CREATE TYPE BODY	81	CREATE TYPE BODY
DECLARE REWRITE EQUIVALENCE	209	DECLARE REWRITE EQUIVALENCE
DISABLE TRIGGER	119	DISABLE TRIGGER
DISASSOCIATE STATISTICS	169	DISASSOCIATE STATISTICS
DROP ASSEMBLY (Release 11.2)	215	DROP ASSEMBLY
DROP CONTEXT	178	DROP CONTEXT
DROP FUNCTION	93	DROP FUNCTION
DROP INDEXTYPE	165	DROP INDEXTYPE
DROP JAVA	162	DROP JAVA
DROP LIBRARY	84	DROP LIBRARY
DROP OPERATOR	167	DROP OPERATOR
DROP PACKAGE	96	DROP PACKAGE
DROP PACKAGE BODY	99	DROP PACKAGE BODY
DROP PROCEDURE	68	DROP PROCEDURE
DROP REWRITE EQUIVALENCE	211	DROP REWRITE EQUIVALENCE
DROP TRIGGER	61	DROP TRIGGER
DROP TYPE	78	DROP TYPE
DROP TYPE BODY	83	DROP TYPE BODY
ENABLE TRIGGER	118	ENABLE TRIGGER
EXECUTE TYPE	123	EXECUTE TYPE
EXPLAIN	50	EXPLAIN

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

Table A-4 Oracle Database Application Management Event Attributes

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

¹ SQL_BIND variable could be truncated to 4000 characters.

² SQL_TEXT variable could be truncated to 4000 characters.

A.4 Audit Command Events

Audit command events track the use of AUDIT SQL statements on other SQL statements and on database objects. The Audit Command Report, described in [Section 3.3.3.3](#), uses these events.

[Table A-5](#) lists the Oracle Database audit command source database events and the equivalent Oracle Audit Vault events.

Table A-5 Oracle Database Audit Command Audit Events

Event Name Description	Source Event	Audit Vault Event
AUDIT DEFAULT	106	AUDIT DEFAULT
AUDIT OBJECT	30	AUDIT OBJECT
NOAUDIT DEFAULT	107	NOAUDIT DEFAULT
NOAUDIT OBJECT	31	NOAUDIT OBJECT
SYSTEM AUDIT	104	SYSTEM AUDIT
SYSTEM NOAUDIT	105	SYSTEM NOAUDIT

[Table A-6](#) lists the Oracle Database audit command event attributes.

Table A-6 Oracle Database Audit Command Event Attributes

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

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

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

¹ SQL_BIND variable could be truncated to 4000 characters.

² SQL_TEXT variable could be truncated to 4000 characters.

A.5 Data Access Events

Data access events track audited data manipulation language (DML) activities, for example, all SELECT, INSERT, UPDATE, or DROP SQL statements. The Data Access Report, described in [Section 3.3.2.3](#), uses these events.

[Table A–7](#) lists the Oracle Database data access source database events and the equivalent Oracle Audit Vault events.

Table A–7 Oracle Database Data Access Audit Events

Event Name Description	Source Event	Audit Vault Event
DELETE	7	DELETE
INSERT	2	INSERT
SELECT	3	SELECT
SELECT MINING MODEL (Release 11.2)	131	SELECT MINING MODEL
TRUNCATE TABLE	85	TRUNCATE TABLE
UPDATE	6	UPDATE

[Table A–8](#) lists the Oracle Database data access event attributes.

Table A–8 Oracle Database Data Access Event Attributes

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

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

Attribute Name	Data Type
COL_NAMELIST	VARCHAR2 (4000)
COL_NEWVAL1	VARCHAR2 (4000)
COL_NEWVAL2	VARCHAR2 (4000)
COL_NEWVAL3	VARCHAR2 (4000)
COL_NEWVAL4	VARCHAR2 (4000)
COL_NEWVAL5	VARCHAR2 (4000)
COL_NEWVAL6	VARCHAR2 (4000)
COL_NEWVAL7	VARCHAR2 (4000)
COL_NEWVAL8	VARCHAR2 (4000)
COL_NEWVAL9	VARCHAR2 (4000)
COL_NEWVAL10	VARCHAR2 (4000)
COL_NEWVAL11	VARCHAR2 (4000)
COL_OLDVAL1	VARCHAR2 (4000)
COL_OLDVAL2	VARCHAR2 (4000)
COL_OLDVAL3	VARCHAR2 (4000)
COL_OLDVAL4	VARCHAR2 (4000)
COL_OLDVAL5	VARCHAR2 (4000)
COL_OLDVAL6	VARCHAR2 (4000)
COL_OLDVAL7	VARCHAR2 (4000)
COL_OLDVAL8	VARCHAR2 (4000)
COL_OLDVAL9	VARCHAR2 (4000)
COL_OLDVAL10	VARCHAR2 (4000)
COL_OLDVAL11	VARCHAR2 (4000)
COMMENT_TEXT	VARCHAR2 (4000)
CONTEXTID	VARCHAR2 (4000)
DATA_VALUES	AV_DATAVALUES_LIST
ENDUSER	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
FGA_POLICYNAME	VARCHAR2 (30)
HOST_IP	VARCHAR2 (255)
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
INSTANCE_NUMBER	NUMBER
NUM_INLINECOL	NUMBER
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2 (4000)

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

Attribute Name	Data Type
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.

A.6 Oracle Database Vault Events

Oracle Database Vault events track audited Oracle Database Vault activity. The Oracle Database Vault Report, described in [Section 3.3.2.4](#), uses these events.

[Table A–9](#) lists the Oracle Database Vault source database events and the equivalent Oracle Audit Vault events.

Table A–9 Oracle Database Vault Audit Events

Event Name Description	Source Event	Audit Vault Event
ACCESS CTRL COMMAND AUTH	1008	ACCESS CTRL COMMAND AUTH
ACCESS CTRL SESSION INIT	1009	ACCESS CTRL SESSION INIT
COMMAND AUTHORIZATION	1005	COMMAND AUTHORIZATION
FACTOR ASSIGNMENT	1001	FACTOR ASSIGNMENT
FACTOR EVALUATION	1000	FACTOR EVALUATION
FACTOR EXPRESSION	1002	FACTOR EXPRESSION
LBL SEC ATTEMPT TO UPGRADE	1010	LBL SEC ATTEMPT TO UPGRADE

Table A–9 (Cont.) Oracle Database Vault Audit Events

Event Name Description	Source Event	Audit Vault Event
LBL SEC SESSION INIT	1007	LBL SEC SESSION INIT
REALM AUTHORIZATION	1004	REALM AUTHORIZATION
REALM VIOLATION	1003	REALM VIOLATION
SECURE ROLE	1006	SECURE ROLE

[Table A–10](#) lists the Oracle Database Vault event attributes.

Table A–10 Oracle Database Vault Event Attributes

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

A.7 Exception Events

Exception events track audited error and exception activity, such as network errors. The Exception Activity Report, described in [Section 3.3.4.2](#), uses these events.

[Table A–11](#) lists the Oracle Database exception source database events and the equivalent Oracle Audit Vault events.

Table A–11 Oracle Database Exception Audit Events

Event Name Description	Source Event	Audit Vault Event
NETWORK ERROR	122	NETWORK ERROR

[Table A–12](#) lists the Oracle Database exception event attributes.

Table A–12 Oracle Database Exception Event Attributes

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

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

Attribute Name	Data Type
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.

A.8 Invalid Record Events

Invalid record events track audited activity that Oracle Audit Vault cannot recognize, possibly due to a corrupted audit record. The Invalid Audit Record Report, described in [Section 3.3.4.3](#), uses these events.

[Table A-13](#) lists the Oracle Database invalid record source database events and the equivalent Oracle Audit Vault events.

Table A-13 Oracle Database Invalid Record Audit Events

Event Name	Description	Source Event	Audit Vault Event
INVALID_RECORD		30000	INVALID_RECORD

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

Table A-14 Oracle Database Invalid Record Event Attributes

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

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

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

¹ SQL_BIND variable could be truncated to 4000 characters.

² SQL_TEXT variable could be truncated to 4000 characters.

A.9 Object Management Events

Object management events track audited actions performed on database objects, such as CREATE TABLE statements. The Object Management Report, described in [Section 3.3.3.4](#), uses these events.

[Table A–15](#) lists the Oracle Database object management source database events and the equivalent Oracle Audit Vault events.

Table A–15 Oracle Database Object Management Audit Events

Event Name Description	Source Event	Audit Vault Event
ALTER DIMENSION	175	ALTER DIMENSION
ALTER EDITION (Release 11.2)	213	ALTER EDITION
ALTER INDEX	11	ALTER INDEX
ALTER MATERIALIZED VIEW	75	ALTER MATERIALIZED VIEW
ALTER MATERIALIZED VIEW LOG	72	ALTER MATERIALIZED VIEW LOG
ALTER MINING MODEL (Release 11.2)	130	ALTER MINING MODEL
ALTER OPERATOR	183	ALTER OPERATOR
ALTER OUTLINE	179	ALTER OUTLINE
ALTER PUBLIC SYNONYM (Release 11.2)	134	ALTER PUBLIC SYNONYM
ALTER SEQUENCE	14	ALTER SEQUENCE
ALTER SYNONYM (Release 11.2)	192	ALTER SYNONYM
ALTER TABLE	15	ALTER TABLE
APPLY TABLE OR SCHEMA POLICY ¹	500	APPLY TABLE OR SCHEMA POLICY
CREATE MINING MODEL (Release 11.2)	133	CREATE MINING MODEL
CREATE DIMENSION	174	CREATE DIMENSION
CREATE DIRECTORY	157	CREATE DIRECTORY
CREATE EDITION (Release 11.2)	212	CREATE EDITION
CREATE INDEX	9	CREATE INDEX
CREATE MATERIALIZED VIEW	74	CREATE MATERIALIZED VIEW
CREATE MATERIALIZED VIEW LOG	71	CREATE MATERIALIZED VIEW LOG

Table A–15 (Cont.) Oracle Database Object Management Audit Events

Event Name Description	Source Event	Audit Vault Event
CREATE OUTLINE	180	CREATE OUTLINE
CREATE PUBLIC DATABASE LINK	112	CREATE PUBLIC DATABASE LINK
CREATE PUBLIC SYNONYM	110	CREATE PUBLIC SYNONYM
CREATE SCHEMA	56	CREATE SCHEMA
CREATE SEQUENCE	13	CREATE SEQUENCE
CREATE SYNONYM	19	CREATE SYNONYM
CREATE TABLE	1	CREATE TABLE
CREATE VIEW	21	CREATE VIEW
DROP DIMENSION	176	DROP DIMENSION
DROP DIRECTORY	158	DROP DIRECTORY
DROP EDITION (Release 11.2)	214	DROP EDITION
DROP INDEX	10	DROP INDEX
DROP MATERIALIZED VIEW	76	DROP MATERIALIZED VIEW
DROP MATERIALIZED VIEW LOG	73	DROP MATERIALIZED VIEW LOG
DROP OUTLINE	181	DROP OUTLINE
DROP PUBLIC DATABASE LINK	113	DROP PUBLIC DATABASE LINK
DROP PUBLIC SYNONYM	111	DROP PUBLIC SYNONYM
DROP SEQUENCE	16	DROP SEQUENCE
DROP SYNONYM	20	DROP SYNONYM
DROP TABLE	12	DROP TABLE
DROP VIEW	22	DROP VIEW
FLASHBACK TABLE	205	FLASHBACK TABLE
LOCK	26	LOCK
PURGE INDEX	201	PURGE INDEX
PURGE TABLE	200	PURGE TABLE
REMOVE TABLE OR SCHEMA POLICY ²	501	REMOVE TABLE OR SCHEMA POLICY
RENAME	28	RENAME
UNDROP OBJECT	202	UNDROP OBJECT
UPDATE INDEXES	182	UPDATE INDEXES
VALIDATE INDEX	23	VALIDATE INDEX

¹ APPLY TABLE OR SCHEMA POLICY is an Oracle Label Security audit event.

² REMOVE TABLE OR SCHEMA POLICY is an Oracle Label Security audit event.

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

Table A–16 Oracle Database Object Management Event Attributes

Attribute Name	Data Type
ASSOCIATED_OBJECT_NAME	VARCHAR2 (4000)

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

Attribute Name	Data Type
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.

A.10 Peer Association Events

Peer association events track database link statements. The Distributed Database Report, described in [Section 3.3.2.5](#), uses these events.

[Table A–17](#) lists the Oracle Database peer association source database events and the equivalent Oracle Audit Vault events.

Table A–17 Oracle Database Peer Association Audit Events

Event Name Description	Source Event	Audit Vault Event
CREATE DATABASE LINK	32	CREATE DATABASE LINK
DROP DATABASE LINK	33	DROP DATABASE LINK

[Table A–18](#) lists the Oracle Database peer association event attributes.

Table A–18 Oracle Database Peer Association Event Attributes

Attribute Name	Data Type
CLIENT_APPINFO	VARCHAR2 (4000)
CLIENT_ID	VARCHAR2 (4000)
COMMENT_TEXT	VARCHAR2 (4000)
CONTEXTID	VARCHAR2 (4000)
ENDUSER	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2 (255)
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
INSTANCE_NUMBER	NUMBER
OBJECT_ID	NUMBER
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 A–18 (Cont.) Oracle Database Peer Association Event Attributes

Attribute Name	Data 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.

A.11 Role and Privilege Management Events

Role and privilege management events track audited role and privilege management activity, such as granting object permissions to a user. The Role and Privilege Management Report, described in [Section 3.3.3.6](#), uses these events.

[Table A–19](#) lists the Oracle Database role and privilege management source database events and the equivalent Oracle Audit Vault events.

Table A–19 Oracle Database Role and Privilege Management Audit Events

Event Name Description	Source Event	Audit Vault Event
ALTER ROLE	79	ALTER ROLE
CREATE ROLE	52	CREATE ROLE
DROP ROLE	54	DROP ROLE
GRANT OBJECT	17	GRANT OBJECT
GRANT ROLE	114	GRANT ROLE
OBJECT EXISTS ERRORS ¹	505	OBJECT EXISTS ERRORS
REVOKE OBJECT	18	REVOKE OBJECT
REVOKE ROLE	115	REVOKE ROLE
SET USER OR PROGRAM UNIT LABEL ¹	502	SET USER OR PROGRAM UNIT LABEL
PRIVILEGED ACTION ¹	506	PRIVILEGED ACTION

¹ OBJECT EXISTS ERRORS, SET USER OR PROGRAM UNIT LABEL, and PRIVILEGED ACTION are Oracle Label Security events.

[Table A–20](#) lists the Oracle Database role and privilege management event attributes.

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

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

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

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

¹ SQL_BIND variable could be truncated to 4000 characters.

² SQL_TEXT variable could be truncated to 4000 characters.

A.12 Service and Application Utilization Events

Service and application utilization events track audited application access activity, such as the execution of PL/SQL procedures or functions. The Procedure Executions Report, described in [Section 3.3.2.6](#), uses these events.

[Table A-21](#) lists the Oracle Database service and application utilization source database events and the equivalent Oracle Audit Vault events.

Table A-21 Oracle Database Service and Application Utilization Audit Events

Event Name Description	Source Event	Audit Vault Event
CALL METHOD	170	CALL METHOD
EXECUTE PROCEDURE	116	EXECUTE PROCEDURE
PL/SQL EXECUTE	47	PL/SQL EXECUTE

[Table A-22](#) lists the Oracle Database service and application utilization event attributes.

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

Attribute Name	Data Type
CLIENT_APPINFO	VARCHAR2 (4000)
CLIENT_ID	VARCHAR2 (4000)
COMMENT_TEXT	VARCHAR2 (4000)
CONTEXTID	VARCHAR2 (4000)
ENDUSER	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2 (255)
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
INSTANCE_NUMBER	NUMBER
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2 (4000)
PARENT_CONTEXTID	VARCHAR2 (4000)
PRIVILEGES_USED	VARCHAR2 (4000)
PROCESS#	NUMBER
PROXY_SESSIONID	NUMBER
SCN	NUMBER
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 A–22 (Cont.) Oracle Database Service and Application Utilization Event Attributes

Attribute Name	Data 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.

A.13 System Management Events

System management events track audited system management activity, such as STARTUP and SHUTDOWN operations. The System Management Report, described in [Section 3.3.3.7](#), uses these events.

[Table A–23](#) lists the Oracle Database system management source database events and the equivalent Oracle Audit Vault events.

Table A–23 Oracle Database System Management Audit Events

Event Name Description	Source Event	Audit Vault Event
ALTER CLUSTER	5	ALTER CLUSTER
ALTER DATABASE	35	ALTER DATABASE
ALTER FLASHBACK ARCHIVE (Release 11.2)	219	ALTER FLASHBACK ARCHIVE
ALTER ROLLBACK SEG	37	ALTER ROLLBACK SEG
ALTER SYSTEM	49	ALTER SYSTEM
ALTER TABLESPACE	40	ALTER TABLESPACE
ANALYZE CLUSTER	64	ANALYZE CLUSTER
CREATE CLUSTER	4	CREATE CLUSTER
CREATE CONTROL FILE	57	CREATE CONTROL FILE
CREATE DATABASE	34	CREATE DATABASE
CREATE FLASHBACK ARCHIVE (Release 11.2)	218	CREATE FLASHBACK ARCHIVE
CREATE ROLLBACK SEG	36	CREATE ROLLBACK SEG
CREATE TABLESPACE	39	CREATE TABLESPACE
DISABLE ALL TRIGGERS	121	DISABLE ALL TRIGGERS
DROP CLUSTER	8	DROP CLUSTER
DROP FLASHBACK ARCHIVE (Release 11.2)	220	DROP FLASHBACK ARCHIVE
DROP ROLLBACK SEG	38	DROP ROLLBACK SEG
DROP TABLESPACE	41	DROP TABLESPACE
ENABLE ALL TRIGGERS	120	ENABLE ALL TRIGGERS
FLASHBACK	128	FLASHBACK
FLASHBACK DATABASE	204	FLASHBACK DATABASE
PURGE DBA_RECYCLEBIN	198	PURGE DBA_RECYCLEBIN

Table A–23 (Cont.) Oracle Database System Management Audit Events

Event Name Description	Source Event	Audit Vault Event
PURGE TABLESPACE	199	PURGE TABLESPACE
SHUTDOWN	20005	SHUTDOWN
STARTUP	20004	STARTUP
SUPER USER TRANSACTION CONTROL (Release 11.2)	20000	SUPER USER TRANSACTION CONTROL
SUPER USER DDL	20002	SUPER USER DDL
SUPER USER DML	20003	SUPER USER DML
SYSTEM GRANT	108	SYSTEM GRANT
SYSTEM REVOKE	109	SYSTEM REVOKE
TRUNCATE CLUSTER	86	TRUNCATE CLUSTER

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

Table A–24 Oracle Database System Management Event Attributes

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

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

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

¹ SQL_BIND variable could be truncated to 4000 characters.

² SQL_TEXT variable could be truncated to 4000 characters.

A.14 Unknown or Uncategorized Events

Unknown or uncategorized events track audited activity that cannot be categorized, such as ALTER SUMMARY statements. The Uncategorized Activity Report, described in [Section 3.3.4.4](#), uses these events.

[Table A–25](#) lists the Oracle Database unknown or uncategorized source database events and the equivalent Oracle Audit Vault events.

Table A–25 Oracle Database Unknown or Uncategorized Audit Events

Event Name Description	Source Event	Audit Vault Event
ALTER SUMMARY	172	ALTER SUMMARY
COMMENT	29	COMMENT
CREATE SUMMARY	171	CREATE SUMMARY
DROP SUMMARY	173	DROP SUMMARY
NO-OP	27	NO-OP
SUPER USER UNKNOWN	20006	SUPER USER UNKNOWN
UNKNOWN	0	UNKNOWN
USER COMMENT	117	USER COMMENT

[Table A–26](#) lists the Oracle Database unknown or uncategorized event attributes.

Table A–26 Oracle Database Unknown or Uncategorized Event Attributes

Attribute Name	Data Type
CLIENT_APPINFO	VARCHAR2 (4000)
CLIENT_ID	VARCHAR2 (4000)
COMMENT_TEXT	VARCHAR2 (4000)
CONTEXTID	VARCHAR2 (4000)
ENDUSER	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)

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

Attribute Name	Data 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.

A.15 User Session Events

User session events track audited authentication events for users who log in to the database. The User Sessions Report, described in [Section 3.3.2.7](#), uses these events.

[Table A–27](#) lists the Oracle Database user session source database events and the equivalent Oracle Audit Vault events.

Table A–27 Oracle Database User Session Audit Events

Event Name Description	Source Event	Audit Vault Event
ALTER SESSION	42	ALTER SESSION
COMMIT	44	COMMIT

Table A–27 (Cont.) Oracle Database User Session Audit Events

Event Name Description	Source Event	Audit Vault Event
CREATE RESTORE POINT	206	CREATE RESTORE POINT
CREATE SESSION	129	CREATE SESSION
DROP RESTORE POINT	207	DROP RESTORE POINT
LOGOFF	101	LOGOFF
LOGOFF BY CLEANUP	102	LOGOFF BY CLEANUP
LOGON	100	LOGON
PROXY AUTHENTICATION ONLY	208	PROXY AUTHENTICATION ONLY
PURGE USER_RECYCLEBIN	197	PURGE USER_RECYCLEBIN
ROLLBACK	45	ROLLBACK
SAVEPOINT	46	SAVEPOINT
SESSION REC	103	SESSION REC
SET ROLE	55	SET ROLE
SET TRANSACTION	48	SET TRANSACTION
SUPER USER LOGON	20001	SUPER USER LOGON

[Table A–28](#) lists the Oracle Database user session event attributes.

Table A–28 Oracle Database User Session Event Attributes

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

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

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

¹ SQL_BIND variable could be truncated to 4000 characters.

² SQL_TEXT variable could be truncated to 4000 characters.

Microsoft SQL Server Audit Events

This appendix contains:

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

B.1 About the Microsoft SQL Server Audit Events

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

- **For alerts.** When you create an alert, you can specify an audit event, based on its category, that can trigger the alert. See ["Creating a Basic Alert"](#) on page 2-30 for more information.
- **For custom reports using third-party tools.** If you want to create custom reports using other Oracle Database reporting products or third-party tools, then refer to the tables in this appendix when you design the reports. See [Chapter 4, "Oracle Audit Vault Data Warehouse Schema"](#) for more information about custom reports created with other tools.

B.2 Account Management Events

Account management events track SQL statements that affect user accounts, such as adding logins or changing login passwords. The Account Management Report, described in [Section 3.3.3.2](#), uses these events.

[Table B–1](#) lists the Microsoft SQL Server account management source database events and the equivalent Oracle Audit Vault events.

Table B–1 SQL Server Account Management Events

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

[Table B–2](#) lists the Microsoft SQL Server account management event attributes.

Table B–2 SQL Server Account Management Event Attributes

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

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

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

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

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

B.3 Application Management Events

Application management events track actions that were performed on the underlying SQL statements, such as creating objects. The Procedure Management Report, described in [Section 3.3.3.5](#), uses these events.

[Table B–3](#) lists the Microsoft SQL Server application management source database events and the equivalent Oracle Audit Vault events.

Table B–3 SQL Server Application Management Audit Events

Event Name Description	Source Event	Audit Vault Event
Audit Database Object Take Ownership Event	DATABASE OBJECT TAKE OWNERSHIP: TRIGGER	ALTER TRIGGER
Audit Schema Object Take Ownership Event	SCHEMA OBJECT TAKE OWNERSHIP: OBJECT	ALTER OBJECT
	SCHEMA OBJECT TAKE OWNERSHIP: PROCEDURE	ALTER PROCEDURE
	SCHEMA OBJECT TAKE OWNERSHIP: TYPE	ALTER TYPE
	SCHEMA OBJECT TAKE OWNERSHIP: TRIGGER	ALTER TRIGGER
Audit Server Object Take Ownership Event	SERVER OBJECT TAKE OWNERSHIP: OBJECT	ALTER OBJECT
Object:Created	OBJECT:CREATED:PROCEDURE	CREATE PROCEDURE
	OBJECT:CREATED:TRIGGER	CREATE TRIGGER
	OBJECT:CREATED:TYPE	
Object:Deleted	OBJECT:DELETED:PROCEDURE	DROP PROCEDURE
	OBJECT:DELETED:TRIGGER	DROP TRIGGER

[Table B–4](#) lists the Microsoft SQL Server application management event attributes.

Table B–4 SQL Server Application Management Event Attributes

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

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

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

B.4 Audit Command Events

Audit command events track the use of audit events, such as altering trace events. The Audit Command Report, described in [Section 3.3.3.3](#), uses these events.

[Table B-5](#) lists the Microsoft SQL Server audit command source database events and the equivalent Oracle Audit Vault events.

Table B-5 SQL Server Audit Command Audit Events

Event Name Description	Source Event	Audit Vault Event
Audit Change Audit Event	CHANGE AUDIT:AUDIT STARTED	SYSTEM AUDIT
	CHANGE AUDIT:AUDIT STOPPED	SYSTEM NOAUDIT
	CHANGE AUDIT:C2 MODE OFF	SYSTEM NOAUDIT
	CHANGE AUDIT:C2 MODE ON	SYSTEM AUDIT
	CHANGE:AUDIT STOPPED	SYSTEM NOAUDIT
	CHANGE:NEW AUDIT STARTED	SYSTEM AUDIT
Audit Server Alter Trace Event	SERVER ALTER TRACE	ALTER TRACE
ExistingConnection	EXISTINGCONNECTION	EXISTING CONNECTION

[Table B-6](#) lists the Microsoft SQL Server audit command events that are logged in the Windows Event Viewer.

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

Source Event	Severity
OP ALTER TRACE: START	10
OP ALTER TRACE: STOP	10

[Table B-7](#) lists the Microsoft SQL Server audit command event attributes.

Table B-7 SQL Server Audit Command Event Attributes

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

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

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

B.5 Data Access Events

The data access event tracks SQL transactions. The Data Access Report, described in [Section 3.3.2.3](#), uses these events.

[Table B-8](#) shows the Microsoft SQL Server data access source event and the equivalent Oracle Audit Vault event.

Table B-8 SQL Server Data Access Audit Events

Event Name Description	Source Event	Audit Vault Event
SQL Transaction	TRANSACTION:BEGIN	SQL-TRANSACTION

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

Table B-9 SQL Server Data Access Event Attributes

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

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

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

B.6 Exception Events

Exception events track audited error and exception activity, such as background job errors. The Exception Activity Report, described in [Section 3.3.4.2](#), uses these events.

[Table B–10](#) lists the Microsoft SQL Server exception source database events and the equivalent Oracle Audit Vault events.

Table B–10 SQL Server Exception Audit Events

Event Name Description	Source Event	Audit Vault Event
Background Job Error	BACKGROUND JOB ERROR:ERROR RETURN	ERROR
	BACKGROUND JOB ERROR:FAILURE	ERROR
	BACKGROUND JOB ERROR:QUEUE IS FULL	ERROR
Blocked Process Report	BLOCKED PROCESS REPORT	ERROR

[Table B–11](#) lists the Microsoft SQL Server exception events that are logged in the Windows Event Viewer.

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

Source Event	Severity	Audit Vault Event
OP ERROR: COMMIT	10	ERROR
OP ERROR: DB OFFLINE	10	ERROR
OP ERROR: MIRRORING ERROR	16	ERROR
OP ERROR: .NET FATAL ERROR	16	ERROR
OP ERROR: .NET USER CODE	16	ERROR
OP ERROR: PROCESS VIOLATION	16	ERROR
OP ERROR: RECOVER	21	ERROR
OP ERROR: RESTORE FAILED	21	ERROR

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

Source Event	Severity	Audit Vault Event
OP ERROR: ROLLBACK	10	ERROR
OP ERROR: SERVER SHUT DOWN	21	ERROR
OP ERROR: STACK OVER FLOW	16	ERROR

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

Table B–12 SQL Server Exception Event Attributes

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

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

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

B.7 Invalid Record Events

Invalid record events track audited activity that Oracle Audit Vault cannot recognize, possibly due to a corrupted audit record. The Invalid Audit Record Report, described in [Section 3.3.4.3](#), uses the invalid record event attributes. (These events do not have any event names; they only contain event attributes.)

[Table B–13](#) lists the Microsoft SQL Server invalid record event attributes.

Table B–13 SQL Server Invalid Record Event Attributes

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

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

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

B.8 Object Management Events

Object management events track audited actions performed on database objects, such as altering an object. The Object Management Report, described in [Section 3.3.3.4](#), uses these events.

[Table B–14](#) lists the Microsoft SQL Server object management source database events and the equivalent Oracle Audit Vault events.

Table B–14 SQL Server Object Management Audit Events

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

Table B–14 (Cont.) SQL Server Object Management Audit Events

Event Name Description	Source Event	Audit Vault Event
Object:Closed	OBJECT:CLOSED	None
Object:Created	OBJECT:CREATED	CREATE OBJECT
	OBJECT:CREATED:COMMIT	COMMIT
	OBJECT:CREATED:INDEX	CREATE INDEX
	OBJECT:CREATED:PROCEDURE	CREATE PROCEDURE
	OBJECT:CREATED:ROLLBACK	ROLLBACK
	OBJECT:CREATED:SCHEMA	CREATE SCHEMA
	OBJECT:CREATED:SYNONYM	CREATE SYNONYM
	OBJECT:CREATED:TABLE	CREATE TABLE
	OBJECT:CREATED:TRIGGER	CREATE TRIGGER
	OBJECT:CREATED:TYPE	CREATE TYPE
OBJECT:CREATED:VIEW	CREATE VIEW	
Object:Deleted	OBJECT:DELETED	DROP OBJECT
	OBJECT:DELETED:COMMIT	COMMIT
	OBJECT:DELETED:INDEX	DROP INDEX
	OBJECT:DELETED:PROCEDURE	DROP PROCEDURE
	OBJECT:DELETED:ROLLBACK	ROLLBACK
	OBJECT:DELETED:SYNONYM	DROP SYNONYM
	OBJECT:DELETED:TABLE	DROP TABLE
	OBJECT:DELETED:TRIGGER	DROP TRIGGER
	OBJECT:DELETED:TYPE	DROP TYPE
OBJECT:DELETED:VIEW	DROP VIEW	

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

Table B–15 SQL Server Object Management Event Attributes

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

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

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

B.9 Peer Association Events

Peer association events track database link statements. The Distributed Database Report, described in [Section 3.3.2.5](#), uses these events. (These events do not have any event names; they only contain event attributes.)

[Table B-16](#) lists the Microsoft SQL Server peer association event attributes.

Table B-16 SQL Server Peer Association Event Attributes

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

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

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

B.10 Role and Privilege Management Events

Role and privilege management events track audited role and privilege management activity, such as granting a user access permission. The Role and Privilege Management Report, described in [Section 3.3.3.6](#), uses these events.

[Table B–17](#) lists the Microsoft SQL Server role and privilege management source database events and the equivalent Oracle Audit Vault events.

Table B–17 SQL Server Role and Privilege Management Audit Events

Event Name Description	Source Event	Audit Vault Event
Audit Add DB User Event	ADD DB USER:GRANT DATABASE ACCESS	GRANT ROLE
	ADD DB USER:GRANTDBACCESS	GRANT ROLE
	ADD DB USER:REVOKE DATABASE ACCESS	REVOKE ROLE
	ADD DB USER:REVOKEDBACCESS	REVOKE ROLE
Audit Add Login to Server Role Event	ADD LOGIN TO SERVER ROLE:ADD	GRANT ROLE
	ADD LOGIN TO SERVER ROLE:DROP	REVOKE ROLE
Audit Add Member to DB Role Event	ADD MEMBER TO DB ROLE:ADD	GRANT ROLE
	ADD MEMBER TO DB ROLE:CHANGE GROUP	ALTER ROLE
	ADD MEMBER TO DB ROLE:DROP	REVOKE ROLE
Audit Add Role Event	ADD ROLE:ADD	GRANT ROLE
	ADD ROLE:DROP	REVOKE ROLE
Audit App Role Change Password Event	APP ROLE CHANGE PASSWORD	ALTER APP ROLE
Audit Database Object GDR Event	DATABASE OBJECT GDR:DENY	DENY OBJECT
	DATABASE OBJECT GDR:GRANT	GRANT OBJECT
	DATABASE OBJECT GDR:REVOKE	REVOKE OBJECT

Table B-17 (Cont.) SQL Server Role and Privilege Management Audit Events

Event Name Description	Source Event	Audit Vault Event
Audit Database Principal Management Event	DATABASE PRINCIPAL MANAGEMENT:ALTER: ROLE	ALTER ROLE
	DATABASE PRINCIPAL MANAGEMENT:CREATE: ROLE	CREATE ROLE
	DATABASE PRINCIPAL MANAGEMENT:DROP: ROLE	DROP ROLE
Audit Login GDR Event	LOGIN GDR:DENY	DENY ROLE
	LOGIN GDR:GRANT	GRANT ROLE
	LOGIN GDR:REVOKE	REVOKE ROLE
Audit Object Derived Permission Event	OBJECT DERIVED PERMISSION:ALTER OBJECT	CHECK PRIVILEGE
	OBJECT DERIVED PERMISSION:CREATE OBJECT	CHECK PRIVILEGE
	OBJECT DERIVED PERMISSION:DROP OBJECT	CHECK PRIVILEGE
	OBJECT DERIVED PERMISSION:DUMP OBJECT	CHECK PRIVILEGE
	OBJECT DERIVED PERMISSION:LOAD OBJECT	CHECK PRIVILEGE
Audit Object GDR Event	OBJECT GDR:DENY	DENY OBJECT
	OBJECT GDR:GRANT	GRANT OBJECT
	OBJECT GDR:REVOKE	REVOKE OBJECT
Audit Object Permission Event	OBJECT PERMISSION	CHECK PRIVILEGE
Audit Server Object GDR Event	SERVER OBJECT GDR:DENY	DENY OBJECT
	SERVER OBJECT GDR:GRANT	GRANT OBJECT
	SERVER OBJECT GDR:REVOKE	REVOKE OBJECT
Audit Server Scope GDR Event	SERVER SCOPE GDR:DENY	DENY ROLE
	SERVER SCOPE GDR:GRANT	GRANT ROLE
	SERVER SCOPE GDR:REVOKE	REVOKE ROLE
Audit Statement GDR Event	STATEMENT GDR:DENY	DENY ROLE
	STATEMENT GDR:GRANT	GRANT ROLE
	STATEMENT GDR:REVOKE	REVOKE ROLE
Audit Statement Permission Event	STATEMENT PERMISSION	CHECK PRIVILEGE

[Table B-18](#) lists the Microsoft SQL Server role and privilege management event attributes.

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

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

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

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

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

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

B.11 Service and Application Utilization Events

Service and application utilization events track audited application access activity. The Procedure Executions Report, described in [Section 3.3.2.6](#), uses these events.

[Table B–19](#) lists the Microsoft SQL Server service and application utilization source database events and the equivalent Oracle Audit Vault events.

Table B–19 SQL Server Service and Application Utilization Audit Events

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

[Table B–20](#) lists the Microsoft SQL Server service and application utilization event attributes.

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

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

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

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

B.12 System Management Events

System management events track audited system management activity, such as backup and restore operations. The System Management Report, described in [Section 3.3.3.7](#), uses these events.

[Table B–21](#) lists the Microsoft SQL Server system management source database events and the equivalent Oracle Audit Vault events.

Table B-21 SQL Server System Management Audit Events

Event Name Description	Source Event	Audit Vault Event
Audit Add DB User Event	ADD DB USER:ADD	ALTER DATABASE
	ADD DB USER:DROP	ALTER DATABASE
	ADD DB USER:SP_ADDUSER	ALTER DATABASE
	ADD DB USER:SP_DROPUSER	ALTER DATABASE
Audit Backup/Restore Event	BACKUP/RESTORE:BACKUP	BACKUP
	BACKUP/RESTORE:BACKUPLOG	BACKUP
	BACKUP/RESTORE:RESTORE	RESTORE
Audit Change Database Owner	CHANGE DATABASE OWNER	ALTER DATABASE
Audit Database Management Event	DATABASE MANAGEMENT:ALTER	ALTER DATABASE
	DATABASE MANAGEMENT:CREATE	CREATE DATABASE
	DATABASE MANAGEMENT:DROP	DROP DATABASE
	DATABASE MANAGEMENT:DUMP	BACKUP
	DATABASE MANAGEMENT:LOAD	RESTORE
Audit Database Object Management Event	DATABASE OBJECT MANAGEMENT:ALTER	ALTER DATABASE
	DATABASE OBJECT MANAGEMENT:CREATE	ALTER DATABASE
	DATABASE OBJECT MANAGEMENT:DROP	ALTER DATABASE
	DATABASE OBJECT MANAGEMENT:DUMP	BACKUP
	DATABASE OBJECT MANAGEMENT:LOAD	RESTORE
	DATABASE OBJECT MANAGEMENT:OPEN	ALTER DATABASE
Audit Database Operation Event	DATABASE OPERATION:SUBSCRIBE TO QUERY NOTIFICATION	QN SUBSCRIPTION
Audit Database Principal Management Event	DATABASE PRINCIPAL MANAGEMENT:DUMP	BACKUP
	DATABASE PRINCIPAL MANAGEMENT:LOAD	RESTORE
Audit DBCC Event	DB CONSISTENCY CHECK	CONSISTENCY CHECK
Audit Schema Object Management Event	SCHEMA OBJECT MANAGEMENT:DUMP	BACKUP
	SCHEMA OBJECT MANAGEMENT:LOAD	RESTORE
Audit Server Object Management Event	SERVER OBJECT MANAGEMENT:ALTER	ALTER SYSTEM
	SERVER OBJECT MANAGEMENT:CREATE	ALTER SYSTEM
	SERVER OBJECT MANAGEMENT:DROP	ALTER SYSTEM
	SERVER OBJECT MANAGEMENT:DUMP	BACKUP
	SERVER OBJECT MANAGEMENT:LOAD	RESTORE
Audit Server Operation Event	SERVER OPERATION:ADMINISTER BULK OPERATIONS	ALTER SYSTEM
	SERVER OPERATION:ALTER RESOURCES	ALTER SYSTEM
	SERVER OPERATION:ALTER SERVER STATE	ALTER SYSTEM
	SERVER OPERATION:ALTER SETTINGS	ALTER SYSTEM
	SERVER OPERATION:AUTHENTICATE	ALTER SYSTEM
	SERVER OPERATION:EXTERNAL ACCESS	ALTER SYSTEM
Audit Server Principal Management Event	SERVER PRINCIPAL MANAGEMENT:DUMP: USER	BACKUP
	SERVER PRINCIPAL MANAGEMENT:LOAD: USER	RESTORE

Table B–21 (Cont.) SQL Server System Management Audit Events

Event Name Description	Source Event	Audit Vault Event
Audit Server Starts and Stops	SERVER STARTS AND STOPS:SHUTDOWN	SHUTDOWN
	SERVER STARTS AND STOPS:STARTED	STARTUP
	SERVER STARTS AND STOPS:PAUSED	SUSPEND
	SERVER STARTS AND STOPS:CONTINUE	RESUME
Audit Server Starts and Stops Event	SERVER STARTS AND STOPS:INSTANCE CONTINUED	RESUME
	SERVER STARTS AND STOPS:INSTANCE PAUSE	SUSPEND
	SERVER STARTS AND STOPS:INSTANCE SHUTDOWN	SHUTDOWN
	SERVER STARTS AND STOPS:INSTANCE STARTED	STARTUP
Database Mirroring State Change	DATABASE MIRRORING STATE CHANGE	MIRRORING STATE CHANGED
Mount Tape	MOUNT TAPE:TAPE MOUNT CANCELLED	MOUNT TAPE
	MOUNT TAPE:TAPE MOUNT COMPLETE	MOUNT TAPE
	MOUNT TAPE:TAPE MOUNT REQUEST	MOUNT TAPE

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

Table B–22 SQL Server System Management Event Attributes

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

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

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

B.13 Unknown or Uncategorized Events

Unknown or uncategorized events track audited activity that cannot be categorized, such as user-created configurations. The Uncategorized Activity Report, described in [Section 3.3.4.4](#), uses these events.

[Table B–23](#) shows the Microsoft SQL Server unknown or uncategorized source database event and the equivalent Oracle Audit Vault event.

Table B–23 SQL Server Unknown or Uncategorized Event Attributes

Event Name Description	Source Event	Audit Vault Event
User Configurable (0-9)	USER CONFIGURABLE	USER CONFIGURABLE
SQL Statement Completed Event	SQL:StmntCompleted	SQL EXECUTION

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

Table B–24 SQL Server Unknown or Uncategorized Event Attributes

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

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

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

B.14 User Session Events

User session events track audited authentication events for users who log in to the database. The User Sessions Report, described in [Section 3.3.2.7](#), uses these events.

[Table B–25](#) lists the Microsoft SQL Server user session source database events and the equivalent Oracle Audit Vault events.

Table B–25 SQL Server User Session Audit Events

Event Name Description	Source Event	Audit Vault Event
Audit Broker Login	BROKER LOGIN:AUTHENTICATION FAILURE	LOGON
	BROKER LOGIN:LOGIN SUCCESS	LOGON
	BROKER LOGIN:LOGIN PROTOCOL ERROR	LOGON
	BROKER LOGIN:MESSAGE FORMAT ERROR	LOGON
	BROKER LOGIN:NEGOTIATE FAILURE	LOGON
Audit Database Mirroring Login Event	DATABASE MIRRORING LOGIN:LOGIN SUCCESS	LOGON
	DATABASE MIRRORING LOGIN:LOGIN PROTOCOL ERROR	
	DATABASE MIRRORING LOGIN:MESSAGE FORMAT ERROR	
	DATABASE MIRRORING LOGIN:NEGOTIATE FAILURE	
	DATABASE MIRRORING LOGIN:AUTHENTICATION FAILURE	
Audit Database Operation Event	DATABASE OPERATION:CHECKPOINT	SAVEPOINT
Audit Database Principal Impersonation Event	DATABASE PRINCIPAL IMPERSONATION	IMPERSONATION
Audit Login	AUDIT LOGIN:LOGIN	LOGON
Audit Login Event	AUDIT LOGIN EVENT:LOGIN	LOGON
Audit Login Failed	AUDIT LOGIN FAILED:LOGIN FAILED	LOGON
Audit Login Failed Event	AUDIT LOGIN FAILED EVENT:LOGIN FAILED	LOGON
Audit Logout	AUDIT LOGOUT:LOGOUT	LOGOFF

Table B–25 (Cont.) SQL Server User Session Audit Events

Event Name Description	Source Event	Audit Vault Event
Audit Logout Event	AUDIT LOGOUT EVENT:LOGOUT	LOGOUT
Audit Server Principal Impersonation Event	SERVER PRINCIPAL IMPERSONATION	IMPERSONATION
SQL Transaction	SQL TRANSACTION:COMMIT	COMMIT
	SQL TRANSACTION:ROLLBACK	ROLLBACK
	SQL TRANSACTION:SAVEPOINT	SAVEPOINT

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

Table B–26 SQL Server User Session Event Attributes

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

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

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

Sybase Adaptive Server Enterprise Audit Events

This appendix contains:

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

C.1 About the Sybase Adaptive Server Enterprise Audit Events

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

- **For alerts.** When you create an alert, you can specify an audit event, based on its category, that can trigger the alert. See ["Creating a Basic Alert"](#) on page 2-30 for more information.
- **For custom reports using third-party tools.** If you want to create custom reports using other Oracle Database reporting products or third-party tools, then refer to the tables in this appendix when you design the reports. See [Chapter 4, "Oracle Audit Vault Data Warehouse Schema"](#) for more information about custom reports created with third-party tools.

C.2 Account Management Events

Account management events track Transact-SQL commands that affect user accounts, such as the `UNLOCK ADMIN ACCOUNT` command. The Account Management Report, described in [Section 3.3.3.2](#), uses these events.

[Table C-1](#) lists the Sybase ASE account management source database events and the equivalent Oracle Audit Vault events.

Table C-1 Sybase ASE Account Management Audit Events

Event Name Description	Source Event	Audit Vault Event
Login Command	CREATE LOGIN COMMAND	CREATE USER
	DROP LOGIN COMMAND	DROP USER
Set SSA Command	SET SSA COMMAND	ALTER USER
SSO Changed Password	SSO CHANGED PASSWORD	ALTER USER
Unlock Admin Account	UNLOCK ADMIN ACCOUNT	ALTER USER

[Table C-2](#) lists the Sybase ASE account management event attributes.

Table C-2 Sybase ASE Account Management Event Attributes

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

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

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

C.3 Application Management Events

Application management events track actions that were performed on the underlying Transact-SQL commands of system services and applications, such as the `CREATE RULE` command. The Procedure Management Report, described in [Section 3.3.3.5](#), uses these events.

[Table C–3](#) lists the Sybase ASE application management source database events and the equivalent Oracle Audit Vault events.

Table C–3 Sybase ASE Application Management Audit Events

Event Name Description	Source Event	Audit Vault Event
Create Default	CREATE DEFAULT	CREATE DEFAULT
Create Message	CREATE MESSAGE	CREATE MESSAGE
Create Procedure	CREATE PROCEDURE	CREATE PROCEDURE
Create Rule	CREATE RULE	CREATE RULE
Create SQLJ Function	CREATE SQLJ FUNCTION	CREATE FUNCTION
Create Trigger	CREATE TRIGGER	CREATE TRIGGER
Drop Default	DROP DEFAULT	DROP DEFAULT
Drop Message	DROP MESSAGE	DROP MESSAGE
Drop Procedure	DROP PROCEDURE	DROP PROCEDURE
Drop Rule	DROP RULE	DROP RULE
Drop SQLJ Function	DROP SQLJ FUNCTION	DROP FUNCTION
Drop Trigger	DROP TRIGGER	DROP TRIGGER

[Table C–4](#) lists the Sybase ASE application management event attributes.

Table C–4 Sybase ASE Application Management Event Attributes

Attribute Name	Data Type
ASSOCIATED_OBJECT_NAME	VARCHAR2 (4000)
ASSOCIATED_OBJECT_OWNER	VARCHAR2 (4000)
COMMENT_TEXT	VARCHAR2 (4000)
CONTEXTID	VARCHAR2 (4000)
CURRENT_VALUE	VARCHAR2 (4000)

Table C-4 (Cont.) Sybase ASE Application Management Event Attributes

Attribute Name	Data Type
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2 (4000)
ENDUSER	VARCHAR2 (4000)
EVENT_MOD	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2 (255)
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
KEYWORD	VARCHAR2 (4000)
NEW_OBJECT_NAME	VARCHAR2 (4000)
NEW_OBJECT_OWNER	VARCHAR2 (4000)
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2 (4000)
PARENT_CONTEXTID	VARCHAR2 (4000)
PREVIOUS_VALUE	VARCHAR2 (4000)
PRIVILEGES_USED	VARCHAR2 (4000)
PROCESS#	NUMBER
PROXY_INFORMATION	VARCHAR2 (4000)
SEQUENCE	VARCHAR2 (4000)
SOURCE_EVENTID	VARCHAR2 (255)
SUB_CONTEXTID	VARCHAR2 (4000)
TARGET_OBJECT	VARCHAR2 (4000)
TARGET_OWNER	VARCHAR2 (4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2 (4000)
USER_GUID	VARCHAR2 (4000)
USERNAME	VARCHAR2 (4000)

C.4 Audit Command Events

Audit command events track the use of auditing Transact-SQL commands on other Transact-SQL commands and on database objects. The Audit Command Report, described in [Section 3.3.3.3](#), uses these events.

[Table C-5](#) lists the Sybase ASE audit command source database events and the equivalent Oracle Audit Vault events.

Table C-5 Sybase ASE Audit Command Audit Events

Event Name Description	Source Event	Audit Vault Event
Auditing Disabled	AUDITING DISABLED	NOAUDIT DEFAULT
Auditing Enabled	AUDITING ENABLED	AUDIT DEFAULT

Table C-6 lists the Sybase ASE audit command event attributes.

Table C-6 Sybase ASE Audit Command Event Attributes

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

C.5 Data Access Events

Data access events track audited Transact-SQL commands, such as all `SELECT TABLE`, `INSERT TABLE`, or `UPDATE TABLE` commands. The Data Access Report, described in [Section 3.3.2.3](#), uses these events.

[Table C-7](#) lists the Sybase ASE data access source database events and the equivalent Oracle Audit Vault events.

Table C-7 Sybase ASE Data Access Audit Events

Event Name Description	Source Event	Audit Vault Event
Access To Audit Table	ACCESS TO AUDIT TABLE	SELECT
BCP In	BCP IN	INSERT
Delete Table	DELETE TABLE	DELETE
Delete View	DELETE VIEW	DELETE
Insert Table	INSERT TABLE	INSERT
Insert View	INSERT VIEW	INSERT
Select Table	SELECT TABLE	SELECT
Select View	SELECT VIEW	SELECT
Truncate Table	TRUNCATE TABLE	TRUNCATE TABLE
Truncation of audit table	TRUNCATION OF AUDIT TABLE	TRUNCATE TABLE
Update Table	UPDATE TABLE	UPDATE
Update View	UPDATE VIEW	UPDATE

[Table C-8](#) lists the Sybase ASE data access event attributes.

Table C-8 Sybase ASE Data Access Event Attributes

Attribute Name	Data Type
COMMENT_TEXT	VARCHAR2 (4000)
CONTEXTID	VARCHAR2 (4000)
CURRENT_VALUE	VARCHAR2 (4000)
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2 (4000)
ENDUSER	VARCHAR2 (4000)
EVENT_MOD	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2 (255)
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
KEYWORD	VARCHAR2 (4000)
OBJECT_ID	NUMBER

Table C–8 (Cont.) Sybase ASE Data Access Event Attributes

Attribute Name	Data Type
OSUSER_NAME	VARCHAR2 (4000)
PARENT_CONTEXTID	VARCHAR2 (4000)
PREVIOUS_VALUE	VARCHAR2 (4000)
PRIVILEGES_USED	VARCHAR2 (4000)
PROCESS#	NUMBER
PROXY_INFORMATION	VARCHAR2 (4000)
SEQUENCE	VARCHAR2 (4000)
SOURCE_EVENTID	VARCHAR2 (255)
SUB_CONTEXTID	VARCHAR2 (4000)
TARGET_OBJECT	VARCHAR2 (4000)
TARGET_OWNER	VARCHAR2 (4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2 (4000)
USER_GUID	VARCHAR2 (4000)
USERNAME	VARCHAR2 (4000)

C.6 Exception Events

Exception events track audited error and exception activity, such as network errors. The Exception Activity Report, described in [Section 3.3.4.2](#), uses these events.

[Table C–9](#) lists Sybase ASE exception source database events and the equivalent Oracle Audit Vault events.

Table C–9 Sybase ASE Exception Audit Events

Event Name Description	Source Event	Audit Vault Event
Fatal Error	FATAL ERROR	FATAL ERROR
Nonfatal Error	NONFATAL ERROR	NONFATAL ERROR

[Table C–10](#) lists the Sybase ASE exception event attributes.

Table C–10 Sybase ASE Exception Event Attributes

Attribute Name	Data Type
COMMENT_TEXT	VARCHAR2 (4000)
CONTEXTID	VARCHAR2 (4000)
CURRENT_VALUE	VARCHAR2 (4000)
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2 (4000)
ENDUSER	VARCHAR2 (4000)
EVENT_MOD	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)

Table C–10 (Cont.) Sybase ASE Exception Event Attributes

Attribute Name	Data Type
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2 (255)
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
KEYWORD	VARCHAR2 (4000)
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2 (4000)
PARENT_CONTEXTID	VARCHAR2 (4000)
PREVIOUS_VALUE	VARCHAR2 (4000)
PRIVILEGES_USED	VARCHAR2 (4000)
PROCESS#	NUMBER
PROXY_INFORMATION	VARCHAR2 (4000)
SEQUENCE	VARCHAR2 (4000)
SOURCE_EVENTID	VARCHAR2 (255)
SUB_CONTEXTID	VARCHAR2 (4000)
TARGET_OBJECT	VARCHAR2 (4000)
TARGET_OWNER	VARCHAR2 (4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2 (4000)
USER_GUID	VARCHAR2 (4000)
USERNAME	VARCHAR2 (4000)

C.7 Invalid Record Events

Invalid record events track audited activity that Oracle Audit Vault cannot recognize, possibly due to a corrupted audit record. The Invalid Audit Record Report, described in [Section 3.3.4.3](#), uses these events.

[Table C–11](#) lists Sybase ASE invalid record event attributes.

Table C–11 Sybase ASE Invalid Record Event Attributes

Attribute Name	Data Type
COMMENT_TEXT	VARCHAR2 (4000)
CONTEXTID	VARCHAR2 (4000)
CURRENT_VALUE	VARCHAR2 (4000)
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2 (4000)
ENDUSER	VARCHAR2 (4000)
ERROR_ID	NUMBER
ERROR_MESSAGE	VARCHAR2 (30)

Table C–11 (Cont.) Sybase ASE Invalid Record Event Attributes

Attribute Name	Data Type
EVENT_MOD	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2 (255)
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
KEYWORD	VARCHAR2 (4000)
MODULE_NAME	VARCHAR2 (100)
OBJECT_ID	NUMBER
ORIGINAL_CONTENT2	VARCHAR2 (4000)
ORIGINAL_CONTENT3	VARCHAR2 (4000)
OSUSER_NAME	VARCHAR2 (4000)
PARENT_CONTEXTID	VARCHAR2 (4000)
PREVIOUS_VALUE	VARCHAR2 (4000)
PRIVILEGES_USED	VARCHAR2 (4000)
PROCESS#	NUMBER
PROXY_INFORMATION	VARCHAR2 (4000)
SEQUENCE	VARCHAR2 (4000)
SEVERITY	NUMBER
SOURCE_EVENTID	VARCHAR2 (255)
SUB_CONTEXTID	VARCHAR2 (4000)
TARGET_OBJECT	VARCHAR2 (4000)
TARGET_OWNER	VARCHAR2 (4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2 (4000)
USER_GUID	VARCHAR2 (4000)
USERNAME	VARCHAR2 (4000)

C.8 Object Management Events

Object management events track audited actions performed on database objects, such as CREATE TABLE commands. The Object Management Report, described in [Section 3.3.3.4](#), uses these events.

[Table C–12](#) lists the Sybase ASE object management source database events and the equivalent Oracle Audit Vault events.

Table C–12 Sybase ASE Object Management Audit Events

Event Name Description	Source Event	Audit Vault Event
Access To Database	ACCESS TO DATABASE	ACCESS DATABASE

Table C–12 (Cont.) Sybase ASE Object Management Audit Events

Event Name Description	Source Event	Audit Vault Event
Alter Table	ALTER TABLE	ALTER TABLE
Bind Default	BIND DEFAULT	ALTER TABLE
Bind Message	BIND MESSAGE	ALTER TABLE
Bind Rule	BIND RULE	ALTER TABLE
Create Index	CREATE INDEX	CREATE INDEX
Create Table	CREATE TABLE	CREATE TABLE
Create View	CREATE VIEW	CREATE VIEW
Drop Index	DROP INDEX	CREATE INDEX
Drop Table	DROP TABLE	DROP TABLE
Drop View	DROP VIEW	DROP VIEW
Unbind Default	UNBIND DEFAULT	ALTER TABLE
Unbind Message	UNBIND MESSAGE	ALTER TABLE
Unbind Rule	UNBIND RULE	ALTER TABLE

[Table C–13](#) lists the Sybase ASE object management event attributes.

Table C–13 Sybase ASE Object Management Event Attributes

Attribute Name	Data Type
ASSOCIATED_OBJECT_NAME	VARCHAR2 (4000)
ASSOCIATED_OBJECT_OWNER	VARCHAR2 (4000)
COMMENT_TEXT	VARCHAR2 (4000)
CONTEXTID	VARCHAR2 (4000)
CURRENT_VALUE	VARCHAR2 (4000)
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2 (4000)
ENDUSER	VARCHAR2 (4000)
EVENT_MOD	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2 (255)
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
KEYWORD	VARCHAR2 (4000)
NEW_OBJECT_NAME	VARCHAR2 (4000)
NEW_OBJECT_OWNER	VARCHAR2 (4000)
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2 (4000)
PARENT_CONTEXTID	VARCHAR2 (4000)

Table C–13 (Cont.) Sybase ASE Object Management Event Attributes

Attribute Name	Data Type
PREVIOUS_VALUE	VARCHAR2 (4000)
PRIVILEGES_USED	VARCHAR2 (4000)
PROCESS#	NUMBER
PROXY_INFORMATION	VARCHAR2 (4000)
SEQUENCE	VARCHAR2 (4000)
SOURCE_EVENTID	VARCHAR2 (255)
SUB_CONTEXTID	VARCHAR2 (4000)
TARGET_OBJECT	VARCHAR2 (4000)
TARGET_OWNER	VARCHAR2 (4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2 (4000)
USER_GUID	VARCHAR2 (4000)
USERNAME	VARCHAR2 (4000)

C.9 Peer Association Events

Peer association events track database link commands. The Distributed Database Report, described in [Section 3.3.2.5](#), uses these events. (These events do not have any event names; they only contain event attributes.)

[Table C–14](#) lists the Sybase ASE peer association event attributes.

Table C–14 Sybase ASE Peer Association Event Attributes

Attribute Name	Data Type
COMMENT_TEXT	VARCHAR2 (4000)
CONTEXTID	VARCHAR2 (4000)
CURRENT_VALUE	VARCHAR2 (4000)
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2 (4000)
ENDUSER	VARCHAR2 (4000)
EVENT_MOD	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2 (255)
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
KEYWORD	VARCHAR2 (4000)
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2 (4000)
PARENT_CONTEXTID	VARCHAR2 (4000)

Table C–14 (Cont.) Sybase ASE Peer Association Event Attributes

Attribute Name	Data Type
PREVIOUS_VALUE	VARCHAR2 (4000)
PRIVILEGES_USED	VARCHAR2 (4000)
PROCESS#	NUMBER
PROXY_INFORMATION	VARCHAR2 (4000)
SEQUENCE	VARCHAR2 (4000)
SOURCE_EVENTID	VARCHAR2 (255)
SUB_CONTEXTID	VARCHAR2 (4000)
TARGET_OBJECT	VARCHAR2 (4000)
TARGET_OWNER	VARCHAR2 (4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2 (4000)
USER_GUID	VARCHAR2 (4000)
USERNAME	VARCHAR2 (4000)

C.10 Role and Privilege Management Events

Role and privilege management events track audited role and privilege management activity, such as revoking permissions from a user to use a specified command. The Role and Privilege Management Report, described in [Section 3.3.3.6](#), uses these events.

[Table C–15](#) lists the Sybase ASE role and privilege management source database events and the equivalent Oracle Audit Vault events.

Table C–15 Sybase ASE Role and Privilege Management Audit Events

Event Name Description	Source Event	Audit Vault Event
Grant Command	GRANT COMMAND	GRANT OBJECT
Revoke Command	REVOKE COMMAND	REVOKE OBJECT
Role Check Performed	ROLE CHECK PERFORMED	CHECK PRIVILEGE
Role Toggling	ROLE TOGGING	SET ROLE
User-defined Function Command	ALTER ROLE FUNCTION EXECUTED	ALTER ROLE
	CREATE ROLE FUNCTION EXECUTED	CREATE ROLE
	DROP ROLE FUNCTION EXECUTED	DROP ROLE
	GRANT ROLE FUNCTION EXECUTED	GRANT ROLE
	REVOKE ROLE FUNCTION EXECUTED	REVOKE ROLE

[Table C–16](#) lists the Sybase ASE role and privilege management event attributes.

Table C–16 Sybase ASE Role and Privilege Management Event Attributes

Attribute Name	Data Type
ADMIN_OPTION	NUMBER
CONTEXTID	VARCHAR2 (4000)
COMMENT_TEXT	VARCHAR2 (4000)

Table C–16 (Cont.) Sybase ASE Role and Privilege Management Event Attributes

Attribute Name	Data Type
CURRENT_VALUE	VARCHAR2 (4000)
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2 (4000)
ENDUSER	VARCHAR2 (4000)
EVENT_MOD	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
GRANTEE	VARCHAR2 (4000)
HOST_IP	VARCHAR2 (255)
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
KEYWORD	VARCHAR2 (4000)
OBJECT_ID	NUMBER
OBJECT_PRIVILEGE	VARCHAR2 (255)
OSUSER_NAME	VARCHAR2 (4000)
PARENT_CONTEXTID	VARCHAR2 (4000)
PREVIOUS_VALUE	VARCHAR2 (4000)
PRIVILEGES_USED	VARCHAR2 (4000)
PROCESS#	NUMBER
PROXY_INFORMATION	VARCHAR2 (4000)
ROLE_NAME	VARCHAR2 (4000)
SEQUENCE	VARCHAR2 (4000)
SOURCE_EVENTID	VARCHAR2 (255)
SUB_CONTEXTID	VARCHAR2 (4000)
SYSTEM_PRIVILEGE	VARCHAR2 (4000)
TARGET_OBJECT	VARCHAR2 (4000)
TARGET_OWNER	VARCHAR2 (4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2 (4000)
USER_GUID	VARCHAR2 (4000)
USERNAME	VARCHAR2 (4000)

C.11 Service and Application Utilization Events

Service and application utilization events track audited application access activity, such as the execution of Transact-SQL commands. The Procedure Executions Report, described in [Section 3.3.2.6](#), uses these events.

[Table C–17](#) lists the Sybase ASE service and application utilization source database events and the equivalent Oracle Audit Vault events.

Table C-17 Sybase ASE Service and Application Utilization Audit Events

Event Name Description	Source Event	Audit Vault Event
Execution Of Stored Procedure	STORED PROCEDURE EXECUTION	EXECUTE PROCEDURE
Execution Of Trigger	TRIGGER EXECUTION	EXECUTE TRIGGER
RPC In	RPC IN	EXECUTE PROCEDURE
RPC Out	RPC OUT	EXECUTE PROCEDURE
Trusted procedure execution	TRUSTED PROCEDURE EXECUTION	EXECUTE PROCEDURE
Trusted trigger execution	TRUSTED TRIGGER EXECUTION	EXECUTE TRIGGER

Table C-18 lists the Sybase ASE service and application utilization event attributes.

Table C-18 Sybase ASE Service and Application Utilization Event Attributes

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

Table C–18 (Cont.) Sybase ASE Service and Application Utilization Event Attributes

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

C.12 System Management Events

System management events track audited system management activity, such as the CREATE DATABASE and DISK INIT commands. The System Management Report, described in [Section 3.3.3.7](#), uses these events.

[Table C–19](#) lists the Sybase ASE system management source database events and the equivalent Oracle Audit Vault events.

Table C–19 Sybase ASE System Management Audit Events

Event Name Description	Source Event	Audit Vault Event
AEK Add Encryption	AEK ADD ENCRYPTION	ALTER SYSTEM
AEK Drop Encryption	AEK DROP ENCRYPTION	ALTER SYSTEM
AEK Key Recovery	AEK KEY RECOVERY	ALTER SYSTEM
AEK Modify Encryption	AEK MODIFY ENCRYPTION	ALTER SYSTEM
AEK Modify Owner	AEK MODIFY OWNER	ALTER SYSTEM
Alter Database	ALTER DATABASE	ALTER DATABASE
Alter Encryption Key	ALTER ENCRYPTION KEY	ALTER SYSTEM
Audit Option Change	AUDIT OPTION CHANGE	AUDIT DEFAULT
Config	CONFIG	ALTER SYSTEM
Create Database	CREATE DATABASE	CREATE DATABASE
Create Encryption Key	CREATE ENCRYPTION KEY	ALTER SYSTEM
DBCC Command	DB CONSISTENCY CHECK	CONSISTENCY CHECK
Deploy UDWS	DEPLOY UDWS	ALTER SYSTEM
Disk Init	DISK INIT	ALTER SYSTEM
Disk Mirror	DISK MIRROR	ALTER SYSTEM
Disk Refit	DISK REFIT	ALTER SYSTEM
Disk Reinit	DISK REINIT	ALTER SYSTEM
Disk Release	DISK RELEASE	ALTER SYSTEM
Disk Remirror	DISK REMIRROR	ALTER SYSTEM
Disk Resize	DISK RESIZE	ALTER SYSTEM
Disk Unmirror	DISK UNMIRROR	ALTER SYSTEM
Drop Database	DROP DATABASE	DROP DATABASE
Drop Encryption Key	DROP ENCRYPTION KEY	ALTER SYSTEM
Dump Database	DUMP DATABASE	BACKUP

Table C–19 (Cont.) Sybase ASE System Management Audit Events

Event Name Description	Source Event	Audit Vault Event
Dump Transaction	DUMP TRANSACTION	BACKUP
Encrypted Column Administration	ENCRYPTED COLUMN ADMINISTRATION	ALTER SYSTEM
kill/terminate Command	KILL/TERMINATE COMMAND	ALTER SYSTEM
Load Database	LOAD DATABASE	RESTORE
Load Transaction	LOAD TRANSACTION	RESTORE
Mount Database	MOUNT DATABASE	ALTER DATABASE
Online Database	ONLINE DATABASE	ALTER DATABASE
Quiesce Database Command	QUIESCE DATABASE COMMAND	ALTER SYSTEM
Server Boot	SERVER BOOT	STARTUP
Server Shutdown	SERVER SHUTDOWN	SHUTDOWN
SSL Administration	SSL ADMINISTRATION	ALTER SYSTEM
Undeploy UDWS	UNDEPLOY UDWS	ALTER SYSTEM
Unmount Database	UNMOUNT DATABASE	ALTER DATABASE

[Table C–20](#) lists the Sybase ASE system management event attributes.

Table C–20 Sybase ASE System Management Event Attributes

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

Table C–20 (Cont.) Sybase ASE System Management Event Attributes

Attribute Name	Data Type
PROXY_INFORMATION	VARCHAR2 (4000)
SEQUENCE	VARCHAR2 (4000)
SOURCE_EVENTID	VARCHAR2 (255)
SUB_CONTEXTID	VARCHAR2 (4000)
TARGET_OBJECT	VARCHAR2 (4000)
TARGET_OWNER	VARCHAR2 (4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2 (4000)
USER_GUID	VARCHAR2 (4000)
USERNAME	VARCHAR2 (4000)

C.13 Unknown or Uncategorized Events

Unknown or uncategorized events track audited activity that cannot be categorized. The Uncategorized Activity Report, described in [Section 3.3.4.4](#), uses these events.

[Table C–21](#) shows the Sybase ASE unknown or uncategorized source database event and the equivalent Oracle Audit Vault event.

Table C–21 Sybase ASE Unknown or Uncategorized Audit Events

Event Name Description	Source Event	Audit Vault Event
Ad Hoc Audit record	AD HOC AUDIT RECORD	UNKNOWN

[Table C–22](#) lists the Sybase ASE unknown or uncategorized event attributes.

Table C–22 Sybase ASE Unknown or Uncategorized Event Attributes

Attribute Name	Data Type
COMMENT_TEXT	VARCHAR2 (4000)
CONTEXTID	VARCHAR2 (4000)
CURRENT_VALUE	VARCHAR2 (4000)
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2 (4000)
ENDUSER	VARCHAR2 (4000)
EVENT_MOD	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2 (255)
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
KEYWORD	VARCHAR2 (4000)
OBJECT_ID	NUMBER

Table C–22 (Cont.) Sybase ASE Unknown or Uncategorized Event Attributes

Attribute Name	Data Type
OSUSER_NAME	VARCHAR2 (4000)
PARENT_CONTEXTID	VARCHAR2 (4000)
PREVIOUS_VALUE	VARCHAR2 (4000)
PRIVILEGES_USED	VARCHAR2 (4000)
PROCESS#	NUMBER
PROXY_INFORMATION	VARCHAR2 (4000)
SEQUENCE	VARCHAR2 (4000)
SOURCE_EVENTID	VARCHAR2 (255)
SUB_CONTEXTID	VARCHAR2 (4000)
TARGET_OBJECT	VARCHAR2 (4000)
TARGET_OWNER	VARCHAR2 (4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2 (4000)
USER_GUID	VARCHAR2 (4000)
USERNAME	VARCHAR2 (4000)

C.14 User Session Events

User session events track audited authentication events for users who log in to the database. The User Sessions Report, described in [Section 3.3.2.7](#), uses these events.

[Table C–23](#) lists the Sybase ASE user session source database events and the equivalent Oracle Audit Vault events.

Table C–23 Sybase ASE User Session Audit Events

Event Name Description	Source Event	Audit Vault Event
Connect to command	CONNECT TO COMMAND	CREATE SESSION
Log In	LOG IN	LOGON
Log Out	LOG OUT	LOGOFF
Setuser Command	SETUSER COMMAND	IMPERSONATION

[Table C–24](#) lists the Sybase ASE user session event attributes.

Table C–24 Sybase ASE User Session Event Attributes

Attribute Name	Data Type
AUTHENTICATION_METHOD	VARCHAR2 (255)
COMMENT_TEXT	VARCHAR2 (4000)
CONTEXTID	VARCHAR2 (4000)
CURRENT_VALUE	VARCHAR2 (4000)
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2 (4000)

Table C-24 (Cont.) Sybase ASE User Session Event Attributes

Attribute Name	Data Type
ENDUSER	VARCHAR2 (4000)
EVENT_MOD	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2 (255)
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
KEYWORD	VARCHAR2 (4000)
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2 (4000)
PARENT_CONTEXTID	VARCHAR2 (4000)
PREVIOUS_VALUE	VARCHAR2 (4000)
PRIVILEGES_USED	VARCHAR2 (4000)
PROCESS#	NUMBER
PROXY_INFORMATION	VARCHAR2 (4000)
SEQUENCE	VARCHAR2 (4000)
SOURCE_EVENTID	VARCHAR2 (255)
SUB_CONTEXTID	VARCHAR2 (4000)
TARGET_OBJECT	VARCHAR2 (4000)
TARGET_OWNER	VARCHAR2 (4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2 (4000)
USER_GUID	VARCHAR2 (4000)
USERNAME	VARCHAR2 (4000)

IBM DB2 Audit Events

This appendix contains:

- [About the IBM DB2 Audit Events](#)
- [Account Management Events](#)
- [Application Management Events](#)
- [Audit Command Events](#)
- [Data Access Events](#)
- [Exception Events](#)
- [Invalid Record Events](#)
- [Object Management Events](#)
- [Peer Association Events](#)
- [Role and Privilege Management Events](#)
- [Service and Application Utilization Events](#)
- [System Management Events](#)
- [Unknown or Uncategorized Events](#)
- [User Session Events](#)

D.1 About the IBM DB2 Audit Events

This appendix lists the audit event names and IDs, and the attribute names and data types for IBM DB2. The audit events are organized by their respective categories (for example, Account Management). You can use these audit events as follows:

- **For alerts.** When you create an alert, you can specify an audit event, based on its category, that can trigger the alert. See ["Creating a Basic Alert"](#) on page 2-30 for more information.
- **For custom reports using third-party tools.** If you want to create custom reports using other Oracle Database reporting products or third-party tools, then refer to the tables in this appendix when you design the reports. See [Chapter 4, "Oracle Audit Vault Data Warehouse Schema"](#) for more information about custom reports created with third-party tools.

D.2 Account Management Events

Account management events track SQL commands that affect user accounts, such as the `UNLOCK ADMIN ACCOUNT` command. The Account Management Report, described in [Section 3.3.3.2](#), uses these events.

[Table D-1](#) lists the IBM DB2 account management source database events and the equivalent Oracle Audit Vault events.

Table D-1 IBM DB2 Account Management Audit Events

Event Name	Description	Source Event	Audit Vault Event
ADD_USER		ADD_USER	CREATE USER
ALTER_USER_ADD_ROLE		ALTER_USER_ADD_ROLE	ALTER USER
ALTER_USER_AUTHENTICATION		ALTER_USER_AUTHENTICATION	ALTER USER
ALTER_USER_DROP_ROLE		ALTER_USER_DROP_ROLE	ALTER USER
DROP_USER		DROP_USER	DROP USER
SET_SESSION_USER		SET_SESSION_USER	ALTER USER

[Table D-2](#) lists the IBM DB2 account management event attributes.

Table D-2 IBM DB2 Account Management Event Attributes

Attribute Name	Data Type
CONTEXTID	VARCHAR2 (4000)
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2 (255)
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
ORIGIN_NODE_NUM	NUMBER
OSUSER_NAME	VARCHAR2 (4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2 (4000)
PRIVILEGES_USED	VARCHAR2 (4000)
PROCESS#	NUMBER
SOURCE_EVENTID	VARCHAR2 (255)
SUB_CONTEXTID	VARCHAR2 (4000)
TARGET_OBJECT	VARCHAR2 (4000)
TARGET_OWNER	VARCHAR2 (4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2 (4000)
TRUSTED_CONTEXT_STR	VARCHAR2

Table D–2 (Cont.) IBM DB2 Account Management Event Attributes

Attribute Name	Data Type
USERNAME	VARCHAR2 (4000)

D.3 Application Management Events

Application management events track actions that were performed on the underlying SQL commands of system services and applications, such as the `CREATE RULE` command. The Procedure Management Report, described in [Section 3.3.3.5](#), uses these events.

[Table D–3](#) lists the IBM DB2 application management source database events and the equivalent Oracle Audit Vault events.

Table D–3 IBM DB2 Application Management Audit Events

Event Name Description	Source Event	Audit Vault Event
ALTER_OBJECT	ALTER_OBJECT	ALTER CONTEXT
		ALTER FUNCTION
		ALTER JAVA
		ALTER PACKAGE
		ALTER PROCEDURE
		ALTER TRIGGER
CREATE_OBJECT	CREATE_OBJECT	CREATE CONTEXT
		CREATE FUNCTION
		CREATE JAVA
		CREATE PACKAGE
		CREATE PROCEDURE
		CREATE TRIGGER
DROP_OBJECT	DROP_OBJECT	DROP CONTEXT
		DROP FUNCTION
		DROP JAVA
		DROP PACKAGE
		DROP PROCEDURE
		DROP TRIGGER

[Table D–4](#) lists the IBM DB2 application management event attributes.

Table D–4 IBM DB2 Application Management Event Attributes

Attribute Name	Data Type
ASSOCIATED_OBJECT_NAME	VARCHAR2 (4000)
ASSOCIATED_OBJECT_OWNER	VARCHAR2 (4000)
CONTEXTID	VARCHAR2 (4000)
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)

Table D–4 (Cont.) IBM DB2 Application Management Event Attributes

Attribute Name	Data Type
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2 (255)
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
ORIGIN_NODE_NUM	NUMBER
NEW_OBJECT_NAME	VARCHAR2 (4000)
NEW_OBJECT_OWNER	VARCHAR2 (4000)
OSUSER_NAME	VARCHAR2 (4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2 (4000)
PRIVILEGES_USED	VARCHAR2 (4000)
PROCESS#	NUMBER
SOURCE_EVENTID	VARCHAR2 (255)
SUB_CONTEXTID	VARCHAR2 (4000)
TARGET_OBJECT	VARCHAR2 (4000)
TARGET_OWNER	VARCHAR2 (4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2 (4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2 (4000)

D.4 Audit Command Events

Audit command events track the use of auditing SQL commands on other SQL commands and on database objects. The Audit Command Report, described in [Section 3.3.3.3](#), uses these events.

[Table D–5](#) lists the IBM DB2 audit command source database events and the equivalent Oracle Audit Vault events.

Table D–5 IBM DB2 Audit Command Audit Events

Event Name	Description	Source Event	Audit Vault Event
AUDIT_REMOVE		AUDIT_REMOVE	NOAUDIT OBJECT
AUDIT_REPLACE		AUDIT_REPLACE	AUDIT
AUDIT_USING		AUDIT_USING	AUDIT
START		START	AUDIT
STOP		STOP	AUDIT

[Table D–6](#) lists the IBM DB2 audit command event attributes.

Table D–6 IBM DB2 Audit Command Event Attributes

Attribute Name	Data Type
AUDIT_OPTION	VARCHAR2 (4000)
CONTEXTID	VARCHAR2 (4000)
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2 (255)
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
ORIGIN_NODE_NUM	NUMBER
OSUSER_NAME	VARCHAR2 (4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2 (4000)
PRIVILEGES_USED	VARCHAR2 (4000)
PROCESS#	NUMBER
SOURCE_EVENTID	VARCHAR2 (255)
SUB_CONTEXTID	VARCHAR2 (4000)
TARGET_OBJECT	VARCHAR2 (4000)
TARGET_OWNER	VARCHAR2 (4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2 (4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2 (4000)

D.5 Data Access Events

Data access events track audited SQL commands, such as all `SELECT TABLE`, `INSERT TABLE`, or `UPDATE TABLE` commands. The Data Access Report, described in [Section 3.3.2.3](#), uses these events.

[Table D–7](#) lists the IBM DB2 data access source database events and the equivalent Oracle Audit Vault events.

Table D–7 IBM DB2 Data Access Audit Events

Event Name	Description	Source Event	Audit Vault Event
EXECUTE		EXECUTE	INSERT UPDATE
STATEMENT		STATEMENT	SELECT

[Table D–8](#) lists the IBM DB2 data access event attributes.

Table D–8 IBM DB2 Data Access Event Attributes

Attribute Name	Data Type
CONTEXTID	VARCHAR2 (4000)
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2 (255)
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
ORIGIN_NODE_NUM	NUMBER
OSUSER_NAME	VARCHAR2 (4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2 (4000)
PRIVILEGES_USED	VARCHAR2 (4000)
PROCESS#	NUMBER
SOURCE_EVENTID	VARCHAR2 (255)
SUB_CONTEXTID	VARCHAR2 (4000)
TARGET_OBJECT	VARCHAR2 (4000)
TARGET_OWNER	VARCHAR2 (4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2 (4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2 (4000)

D.6 Exception Events

Exception events track audited error and exception activity, such as network errors. The Exception Activity Report, described in [Section 3.3.4.2](#), uses these events. These events do not have any event names; they only contain event attributes.

[Table D–9](#) lists the IBM DB2 exception event attributes.

Table D–9 IBM DB2 Exception Event Attributes

Attribute Name	Data Type
CONTEXTID	VARCHAR2 (4000)
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2 (255)

Table D–9 (Cont.) IBM DB2 Exception Event Attributes

Attribute Name	Data Type
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
ORIGIN_NODE_NUM	NUMBER
OSUSER_NAME	VARCHAR2 (4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2 (4000)
PRIVILEGES_USED	VARCHAR2 (4000)
PROCESS#	NUMBER
SOURCE_EVENTID	VARCHAR2 (255)
SUB_CONTEXTID	VARCHAR2 (4000)
TARGET_OBJECT	VARCHAR2 (4000)
TARGET_OWNER	VARCHAR2 (4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2 (4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2 (4000)

D.7 Invalid Record Events

Invalid record events track audited activity that Oracle Audit Vault cannot recognize, possibly due to a corrupted audit record. The Invalid Audit Record Report, described in [Section 3.3.4.3](#), uses these events.

[Table D–10](#) lists IBM DB2 invalid record event attributes.

Table D–10 IBM DB2 Invalid Record Event Attributes

Attribute Name	Data Type
CONTEXTID	VARCHAR2 (4000)
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2 (4000)
ERROR_ID	NUMBER
ERROR_MESSAGE	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2 (255)
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
MODULE_NAME	VARCHAR2 (4000)
ORIGIN_NODE_NUM	NUMBER
ORIGINAL_CONTEXT1	VARCHAR2 (4000)

Table D–10 (Cont.) IBM DB2 Invalid Record Event Attributes

Attribute Name	Data Type
ORIGINAL_CONTEXT2	VARCHAR2 (4000)
ORIGINAL_CONTEXT3	VARCHAR2 (4000)
OSUSER_NAME	VARCHAR2 (4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2 (4000)
PRIVILEGES_USED	VARCHAR2 (4000)
PROCESS#	NUMBER
SEVERITY	NUMBER
SOURCE_EVENTID	VARCHAR2 (255)
SUB_CONTEXTID	VARCHAR2 (4000)
TARGET_OBJECT	VARCHAR2 (4000)
TARGET_OWNER	VARCHAR2 (4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2 (4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2 (4000)

D.8 Object Management Events

Object management events track audited actions performed on database objects, such as `CREATE TABLE` commands. The Object Management Report, described in [Section 3.3.3.4](#), uses these events.

[Table D–11](#) lists the IBM DB2 object management source database events and the equivalent Oracle Audit Vault events.

Table D–11 IBM DB2 Object Management Audit Events

Event Name	Description	Source Event	Audit Vault Event
ALTER_OJBECT		ALTER_OBJECT	ALTER INDEX
			ALTER OBJECT
			ALTER SCHEMA
			ALTER SEQUENCE
			ALTER TABLE
			ALTER VIEW
CREATE_OBJECT		CREATE_OBJECT	CREATE INDEX
			CREATE OBJECT
			CREATE SCHEMA
			CREATE SEQUENCE
			CREATE TABLE
			CREATE VIEW

Table D–11 (Cont.) IBM DB2 Object Management Audit Events

Event Name	Description	Source Event	Audit Vault Event
DROP_OBJECT		DROP_OBJECT	DROP INDEX
			DROP OBJECT
			DROP SCHEMA
			DROP SEQUENCE
			DROP TABLE
			DROP VIEW
RENAME_OBJECT		RENAME_OBJECT	RENAME

Table D–12 lists the IBM DB2 object management event attributes.

Table D–12 IBM DB2 Object Management Event Attributes

Attribute Name	Data Type
ASSOCIATED_OBJECT_NAME	VARCHAR2 (4000)
ASSOCIATED_OBJECT_OWNER	VARCHAR2 (4000)
CONTEXTID	VARCHAR2 (4000)
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2 (255)
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
NEW_OBJECT_NAME	VARCHAR2 (4000)
NEW_OBJECT_OWNER	VARCHAR2 (4000)
ORIGIN_NODE_NUM	NUMBER
OSUSER_NAME	VARCHAR2 (4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2 (4000)
PRIVILEGES_USED	VARCHAR2 (4000)
PROCESS#	NUMBER
SOURCE_EVENTID	VARCHAR2 (255)
SUB_CONTEXTID	VARCHAR2 (4000)
TARGET_OBJECT	VARCHAR2 (4000)
TARGET_OWNER	VARCHAR2 (4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2 (4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2 (4000)

D.9 Peer Association Events

Peer association events track database link commands. The Distributed Database Report, described in [Section 3.3.2.5](#), uses these events. These events do not have any event names; they only contain event attributes.

[Table D–13](#) lists the IBM DB2 peer association event attributes.

Table D–13 IBM DB2 Peer Association Event Attributes

Attribute Name	Data Type
CONTEXTID	VARCHAR2 (4000)
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2 (255)
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
ORIGIN_NODE_NUM	NUMBER
OSUSER_NAME	VARCHAR2 (4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2 (4000)
PRIVILEGES_USED	VARCHAR2 (4000)
PROCESS#	NUMBER
SOURCE_EVENTID	VARCHAR2 (255)
SUB_CONTEXTID	VARCHAR2 (4000)
TARGET_OBJECT	VARCHAR2 (4000)
TARGET_OWNER	VARCHAR2 (4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2 (4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2 (4000)

D.10 Role and Privilege Management Events

Role and privilege management events track audited role and privilege management activity, such as granting a user permissions to alter an object. The Role and Privilege Management Report, described in [Section 3.3.3.6](#), uses these events.

[Table D–14](#) lists the IBM DB2 role and privilege management source database events and the equivalent Oracle Audit Vault events.

Table D–14 IBM DB2 Role and Privilege Management Audit Events

Event Name	Description	Source Event	Audit Vault Event
ALTER_OBJECT		ALTER_OBJECT	ALTER_ROLE

Table D–14 (Cont.) IBM DB2 Role and Privilege Management Audit Events

Event Name Description	Source Event	Audit Vault Event
CHECKING_FUNCTION	CHECKING_FUNCTION	CHECK PRIVILEGE
CHECKING_OBJECT	CHECKING_OBJECT	CHECK PRIVILEGE
CREATE_OBJECT	CREATE_OBJECT	CREATE ROLE
DROP_OBJECT	DROP_OBJECT	DROP ROLE
GRANT	GRANT	GRANT OBJECT GRANT ROLE
GRANT_DB_AUTHORITIES	GRANT_DB_AUTHORITIES	SYSTEM GRANT
GRANT_DBADM	GRANT_DBADM	GRANT OBJECT
IMPLICIT_GRANT	IMPLICIT_GRANT	GRANT OBJECT
IMPLICIT_REVOKE	IMPLICIT_REVOKE	REVOKE OBJECT
REVOKE	REVOKE	REVOKE OBJECT REVOKE ROLE
REVOKE_DB_AUTHORITIES	REVOKE_DB_AUTHORITIES	SYSTEM REVOKE
REVOKE_DBADM	REVOKE_DBADM	REVOKE OBJECT
TRANSFER_OWNERSHIP	TRANSFER_OWNERSHIP	GRANT ROLE

Table D–15 lists the IBM DB2 role and privilege management event attributes.

Table D–15 IBM DB2 Role and Privilege Management Event Attributes

Attribute Name	Data Type
ADMIN_OPTION	NUMBER
CONTEXTID	VARCHAR2 (4000)
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
GRANTEE	VARCHAR2 (4000)
HOST_IP	VARCHAR2 (255)
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
OBJECT_PRIVILEGE	VARCHAR2 (4000)
ORIGIN_NODE_NUM	NUMBER
OSUSER_NAME	VARCHAR2 (4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2 (4000)
PRIVILEGES_USED	VARCHAR2 (4000)
PROCESS#	NUMBER
ROLE_NAME	VARCHAR2 (4000)

Table D–15 (Cont.) IBM DB2 Role and Privilege Management Event Attributes

Attribute Name	Data Type
SOURCE_EVENTID	VARCHAR2 (255)
SUB_CONTEXTID	VARCHAR2 (4000)
SYSTEM_PRIVILEGE	VARCHAR2 (4000)
TARGET_OBJECT	VARCHAR2 (4000)
TARGET_OWNER	VARCHAR2 (4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2 (4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2 (4000)

D.11 Service and Application Utilization Events

Service and application utilization events track audited application access activity, such as the execution of SQL commands. The Procedure Executions Report, described in [Section 3.3.2.6](#), uses these events.

[Table D–16](#) lists the IBM DB2 service and application utilization source database events and the equivalent Oracle Audit Vault events.

Table D–16 IBM DB2 Service and Application Utilization Audit Events

Event Name	Description	Source Event	Audit Vault Event
EXECUTE		EXECUTE	PL/SQL EXECUTE
EXECUTE_IMMEDIATE		EXECUTE_IMMEDIATE	PL/SQL EXECUTE

[Table D–17](#) lists the IBM DB2 service and application utilization event attributes.

Table D–17 IBM DB2 Service and Application Utilization Event Attributes

Attribute Name	Data Type
CONTEXTID	VARCHAR2 (4000)
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2 (255)
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
ORIGIN_NODE_NUM	NUMBER
OSUSER_NAME	VARCHAR2 (4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2 (4000)
PRIVILEGES_USED	VARCHAR2 (4000)

Table D–17 (Cont.) IBM DB2 Service and Application Utilization Event Attributes

Attribute Name	Data Type
PROCESS#	NUMBER
SOURCE_EVENTID	VARCHAR2 (255)
SUB_CONTEXTID	VARCHAR2 (4000)
TARGET_OBJECT	VARCHAR2 (4000)
TARGET_OWNER	VARCHAR2 (4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2 (4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2 (4000)

D.12 System Management Events

System management events track audited system management activity, such as the CREATE DATABASE and DISK INIT commands. The System Management Report, described in [Section 3.3.3.7](#), uses these events.

[Table D–18](#) lists the IBM DB2 system management source database events and the equivalent Oracle Audit Vault events.

Table D–18 IBM DB2 System Management Audit Events

Event Name Description	Source Event	Audit Vault Event
ACTIVATE_DB	ACTIVATE_DB	ALTER DATABASE
ADD_NODE	ADD_NODE	CREATE NODE
ALTER_BUFFERPOOL	ALTER_BUFFERPOOL	ALTER_BUFFERPOOL
ALTER_DATABASE	ALTER_DATABASE	ALTER DATABASE
ALTER_NODEGROUP	ALTER_NODEGROUP	ALTER_NODEGROUP
ALTER_OBJECT	ALTER_OBJECT	ALTER TABLESPACE
ALTER_TABLESPACE	ALTER_TABLESPACE	ALTER TABLESPACE
BACKUP_DB	BACKUP_DB	BACKUP
BIND	BIND	ALTER DATABASE
CLOSE_HISTORY_FILE	CLOSE_HISTORY_FILE	ALTER SYSTEM
CONFIGURE	CONFIGURE	ALTER SYSTEM
CREATE_BUFFERPOOL	CREATE_BUFFERPOOL	CREATE_BUFFERPOOL
CREATE_DATABASE	CREATE_DATABASE	CREATE DATABASE
CREATE_DB_AT_NODE	CREATE_DB_AT_NODE	CREATE DATABASE
CREATE_EVENT_MONITOR	CREATE_EVENT_MONITOR	CREATE_EVENT_MONITOR
CREATE_INSTANCE	CREATE_INSTANCE	CREATE_INSTANCE
CREATE_NODEGROUP	CREATE_NODEGROUP	CREATE_NODEGROUP
CREATE_OBJECT	CREATE_OBJECT	CREATE TABLESPACE
CREATE_TABLESPACE	CREATE_TABLESPACE	CREATE TABLESPACE

Table D–18 (Cont.) IBM DB2 System Management Audit Events

Event Name Description	Source Event	Audit Vault Event
DB2AUDIT	DB2AUDIT	ALTER SYSTEM
DB2REMOT	DB2REMOT	DB2REMOT
DB2SET	DB2SET	ALTER SYSTEM
DEACTIVATE_DB	DEACTIVATE_DB	ALTER DATABASE
DELETE_INSTANCE	DELETE_INSTANCE	DELETE_INSTANCE
DROP_BUFFERPOOL	DROP_BUFFERPOOL	DROP_BUFFERPOOL
DROP_DATABASE	DROP_DATABASE	DROP DATABASE
DROP_EVENT_MONITOR	DROP_EVENT_MONITOR	DROP_EVENT_MONITOR
DROP_NODEGROUP	DROP_NODEGROUP	DROP_NODEGROUP
DROP_OBJECT	DROP_OBJECT	DROP TABLESPACE
DROP_TABLESPACE	DROP_TABLESPACE	DROP TABLESPACE
FETCH_HISTORY_FILE	FETCH_HISTORY_FILE	ALTER SYSTEM
FORCE_APPLICATION	FORCE_APPLICATION	FORCE_APPLICATION
KILLDBM	KILLDBM	ALTER SYSTEM
MIGRATE_DB	MIGRATE_DB	ALTER SYSTEM
MIGRATE_DB_DIR	MIGRATE_DB_DIR	ALTER SYSTEM
MIGRATE_SYSTEM_DIRECTORY	MIGRATE_SYSTEM_DIRECTORY	ALTER SYSTEM
OPEN_HISTORY_FILE	OPEN_HISTORY_FILE	ALTER SYSTEM
QUIESCE_TABLESPACE	QUIESCE_TABLESPACE	ALTER TABLESPACE
REBIND	REBIND	ALTER DATABASE
RENAME_TABLESPACE	RENAME_TABLESPACE	ALTER TABLESPACE
RESET_ADMIN_CFG	RESET_ADMIN_CFG	ALTER SYSTEM
RESET_DB_CFG	RESET_DB_CFG	ALTER DATABASE
RESET_DBM_CFG	RESET_DBM_CFG	ALTER SYSTEM
RESTORE_DB	RESTORE_DB	RESTORE
ROLLFORWARD_DB	ROLLFORWARD_DB	ROLLFORWARD
SET_APPL_PRIORITY	SET_APPL_PRIORITY	ALTER SYSTEM
SET_TABLESPACE_CONTAINERS	SET_TABLESPACE_CONTAINERS	ALTER TABLESPACE
START_DB2	START_DB2	STARTUP
STOP_DB2	STOP_DB2	SHUTDOWN
UNQUIESCE_TABLESPACE	UNQUIESCE_TABLESPACE	ALTER TABLESPACE
UPDATE_ADMIN_CFG	UPDATE_ADMIN_CFG	ALTER SYSTEM
UPDATE_AUDIT	UPDATE_AUDIT	ALTER SYSTEM
UPDATE_DB_CFG	UPDATE_DB_CFG	ALTER DATABASE
UPDATE_DBM_CFG	UPDATE_DBM_CFG	ALTER SYSTEM

[Table D–19](#) lists the IBM DB2 system management event attributes.

Table D–19 IBM DB2 System Management Event Attributes

Attribute Name	Data Type
CONTEXTID	VARCHAR2 (4000)
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2 (255)
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
ORIGIN_NODE_NUM	NUMBER
OSUSER_NAME	VARCHAR2 (4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2 (4000)
PRIVILEGES_USED	VARCHAR2 (4000)
PROCESS#	NUMBER
SOURCE_EVENTID	VARCHAR2 (255)
SUB_CONTEXTID	VARCHAR2 (4000)
TARGET_OBJECT	VARCHAR2 (4000)
TARGET_OWNER	VARCHAR2 (4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2 (4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2 (4000)

D.13 Unknown or Uncategorized Events

Unknown or uncategorized events track audited activity that cannot be categorized. The Uncategorized Activity Report, described in [Section 3.3.4.4](#), uses these events.

[Table D–20](#) lists the IBM DB2 unknown or uncategorized source database event and equivalent Oracle Audit Vault event.

Table D–20 IBM DB2 Unknown or Uncategorized Audit Events

Event Name Description	Source Event	Audit Vault Event
ALTER_OBJECT	ALTER_OBJECT	ALTER SUMMARY
CREATE_OBJECT	CREATE_OBJECT	CREATE SUMMARY
DROP_OBJECT	DROP_OBJECT	DROP SUMMARY

[Table D–21](#) lists the IBM DB2 unknown or uncategorized event attributes.

Table D–21 IBM DB2 Unknown or Uncategorized Event Attributes

Attribute Name	Data Type
CONTEXTID	VARCHAR2 (4000)
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2 (255)
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
ORIGIN_NODE_NUM	NUMBER
OSUSER_NAME	VARCHAR2 (4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2 (4000)
PRIVILEGES_USED	VARCHAR2 (4000)
PROCESS#	NUMBER
SOURCE_EVENTID	VARCHAR2 (255)
SUB_CONTEXTID	VARCHAR2 (4000)
TARGET_OBJECT	VARCHAR2 (4000)
TARGET_OWNER	VARCHAR2 (4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2 (4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2 (4000)

D.14 User Session Events

User session events track audited authentication events for users who log in to the database. The User Sessions Report, described in [Section 3.3.2.7](#), uses these events.

[Table D–22](#) lists the IBM DB2 user session source database events and the equivalent Oracle Audit Vault events.

Table D–22 IBM DB2 User Session Audit Events

Event Name Description	Source Event	Audit Vault Event
ATTACH	ATTACH	CREATE SESSION
AUTHENTICATE	AUTHENTICATE	AUTHENTICATE
COMMIT	COMMIT	COMMIT
CONNECT	CONNECT	LOGON
CONNECT RESET	CONNECT RESET	LOGOFF
DETACH	DETACH	ALTER SESSION

Table D–22 (Cont.) IBM DB2 User Session Audit Events

Event Name	Description	Source Event	Audit Vault Event
ROLLBACK		ROLLBACK	ROLLBACK
VALIDATE_USER		VALIDATE_USER	AUTHENTICATE

Table D–23 lists the IBM DB2 user session event attributes.

Table D–23 IBM DB2 User Session Event Attributes

Attribute Name	Data Type
AUTHENTICATION_METHOD	VARCHAR2 (255)
CONTEXTID	VARCHAR2 (4000)
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2 (4000)
EVENT_STATUS	VARCHAR2 (30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2 (255)
HOST_NAME	VARCHAR2 (255)
HOST_TERMINAL	VARCHAR2 (255)
ORIGIN_NODE_NUM	NUMBER
OSUSER_NAME	VARCHAR2 (4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2 (4000)
PRIVILEGES_USED	VARCHAR2 (4000)
PROCESS#	NUMBER
SOURCE_EVENTID	VARCHAR2 (255)
SUB_CONTEXTID	VARCHAR2 (4000)
TARGET_OBJECT	VARCHAR2 (4000)
TARGET_OWNER	VARCHAR2 (4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2 (4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2 (4000)

Index

A

access reports

See reports, default access

account management events

Account Management Report, 3-6

IBM DB2, D-2

Oracle Database, A-2

SQL Server, B-2

Sybase Adaptive Server Enterprise, C-2

Activity Overview Report, 3-4

Adaptive Server Enterprise

See Sybase Adaptive Server Enterprise

administrative changes

checking collection agent status, 1-8

alerts

about, 2-21

activity summary, 2-37

advanced using condition and function, 2-35

advanced using condition only, 2-32

application users, example of creating alerts for, 2-33

creating advanced alerts with condition and alert, 2-35

creating advanced alerts with condition only, 2-32

creating alert status values, 2-29

creating basic alerts, 2-30

creating rules, 2-22, 2-24, 2-27, 2-29, 2-30

how they are raised, 2-36

listing, 2-30

monitoring, 2-36

reports, 3-15

responding to, 2-38

All Alerts Report, 3-15

annotating reports, 3-18

application management events

IBM DB2, D-3

Oracle Database, A-3

Procedure Management Report, 3-7

SQL Server, B-4

Sybase Adaptive Server Enterprise, C-3

application users, example of creating alerts for, 2-33

ASE

See Sybase Adaptive Server Enterprise

attesting to reports, 3-18

procedure for auditors, 3-18

specifying auditor list, 3-16

audit command events

Audit Commands Report, 3-6

IBM DB2, D-4

Oracle Database, A-6

SQL Server, B-6

Sybase Adaptive Server Enterprise, C-4

Audit Commands Report, 3-6

audit events

context information in CONTEXT_DIM dimension table, 4-4

IBM DB2, listed, D-1 to D-17

information in EVENT_DIM dimension table, 4-4

Oracle Database, A-1 to A-25

Oracle Database Vault, A-9

SQL Server, B-1 to B-28

Sybase Adaptive Server Enterprise, C-1 to C-19

See also reports

audit policies

about, 2-1

activating, 2-4

copying to another database, 2-21

creating, general tasks for, 2-2

fine-grained auditing, 2-12

privilege auditing, 2-10

provisioning to source database, 2-19

redo log files, capture rules for, 2-17

retrieving, 2-2

schema object auditing, 2-8

source database, retrieving settings from, 2-2

SQL statement auditing, 2-5

verifying semantic correctness, 2-19

audit policy settings

manually provisioning to source database, 2-20

saving to SQL script, 2-20

audit records

finding information about, 3-33

setting a retention period for audit data, 2-39

what happens when collection agents not active, 1-9

audit settings

recommended for Oracle source database, 1-5

refreshing audit settings state, 2-4

retention period for audit data, 2-39

source database settings, retrieving, 2-4

- updating state, 2-4
- Audit Settings Changes Report, 3-13
- Audit Vault Console
 - creating alert rules, 2-21
 - monitoring alerts from, 2-21
 - starting, 1-6
- AUDIT_EVENT_FACT fact table
 - contents of, 4-7
- audited data
 - types of, 1-2
- auditing
 - enabling in source database, 1-4
 - fine-grained, 2-12
 - general tasks, 1-2
 - privileges, 2-10
 - redo log files, 2-17
 - schema objects, 2-8
 - SQL statements, 2-5
- AV\$DW_BEFORE_AFTER PL/SQL package, 4-18

B

- before and after values
 - accessing from redo logs, 4-18
 - AV\$DW_BEFORE_AFTER PL/SQL package, 4-18
 - Before/After Values Report, 3-13
 - creating capture rules for, 2-17
- Before/After Values Report, 3-13

C

- capture rules
 - See* redo log file auditing
- categories
 - creating for user-defined reports, 3-34
- changed data, finding and comparing
 - See* entitlement report snapshots and labels, 3-19
- changes to audit events
 - Audit Setting Changes Report, 3-13
- Changes to Audit Report, 3-13
- charting data in reports, 3-31
- client connections
 - information in CLIENT_HOST_DIM dimension table, 4-4
 - tool information in CLIENT_TOOLS_DIM dimension table, 4-4
- CLIENT_HOST_DIM dimension table
 - about, 4-4
 - contents of, 4-13
- CLIENT_TOOL_DIM dimension table
 - about, 4-4
 - contents of, 4-13
- collection agents
 - checking status of, 1-8
- columns in a report
 - See also* relevant columns
- columns in report
 - finding information about, 3-33
 - hiding current column, 3-24

- hiding or showing, 3-25
- comparing snapshot or label audit data, 3-23
- compliance reports
 - See* reports, compliance
- CONTEXT_DIM dimension table
 - about, 4-4
 - contents of, 4-13
- credit card compliance report
 - Credit Card Related Data Access Report, 3-12
- Credit Card Related Data Access Report, 3-12
- credit card reports
 - See* compliance reports, Credit Card Related Data Access Report
- Critical Alerts Report, 3-15
- CSV files, saving reports to, 3-36
- custom reports
 - See* data warehouse schema

D

- Dashboard page
 - alert monitoring, 2-36
 - displaying, 2-36
- data access events
 - Data Access Report, 3-4
 - IBM DB2, D-5
 - Oracle Database, A-7
 - Oracle Database Vault, A-9
 - report, 3-12, 3-13
 - SQL Server, B-7
 - Sybase Adaptive Server Enterprise, C-6
- Data Access Report, 3-4
- data warehouse schema
 - about, 4-1
 - architecture, 4-1
 - AUDIT_EVENT_FACT table, 4-7
 - CLIENT_HOST_DIM table, 4-4, 4-13
 - CLIENT_TOOL_DIM table, 4-4, 4-13
 - CONTEXT_DIM table, 4-4, 4-13
 - design, 4-2
 - dimension tables
 - about, 4-3
 - relationships, 4-6
 - EVENT_DIM table, 4-4, 4-14
 - fact tables
 - about, 4-3
 - constraints, 4-5
 - indexes, 4-5
 - relationships, 4-6
 - used in data warehouse schema, 4-3
 - PRIVILEGES_DIM table, 4-5, 4-14
 - SOURCE_DIM table, 4-5, 4-15
 - TARGET_DIM table, 4-4, 4-15
 - TIME_DIM table, 4-4, 4-16
 - USER_DIM table, 4-4, 4-18
- data, changed by INSERT, UPDATE, DELETE
 - Program Changes Report, 3-14
- Database Failed Logins Report, 3-14
- Database Login/Logoff Report, 3-14
- Database Logoff Report, 3-14

- Database Logon Report, 3-14
- Database Roles by Source Report, 3-10
- Database Roles Report, 3-10
- Database Startup/Shutdown Report, 3-14
- Database Vault
 - See Oracle Database Vault
- Database Vault Report, 3-5
- databases
 - audit policies
 - copying to another database, 2-21
 - provisioning to source database, 2-19
 - retrieving from, 2-2
 - Database Roles Report, 3-10
 - distributed
 - tracking with Distributed Database Report, 3-5
 - logon operations, report, 3-14
 - monitoring source database, 1-8
 - requirements for auditing, 1-4
 - source database information in SOURCE_DIM dimension table, 4-5
 - startup and shutdown operations, report, 3-14
- DDL report audit events
 - Schema Changes Report, 3-14
- default access reports
 - See reports, default access
- default entitlement reports
 - See reports, default entitlement
- default management activity reports
 - See reports, default management activity
- default settings in reports
 - reverting to, 3-33
- default system exception reports
 - See reports, default system exception
- Deleted Objects Report, 3-14
- dimension tables
 - See data warehouse schema
- dimension, used in data warehouse schema, 4-3
- Distributed Database Report, 3-5

E

- e-mail notifications
 - about, 2-22
 - creating a notification template, 2-23
 - creating a profile, 2-22
 - creating for alerts, 2-38
 - list for reports, 3-16
- entitlement report snapshots and labels
 - about, 3-19
 - general steps for using, 3-19
 - assigning snapshots to a label, 3-21
 - comparing snapshot or label data, 3-23
 - creating label, 3-20
 - generating individual snapshot or label data, 3-22
 - retrieving entitlement audit data, 3-20
 - viewing snapshot and label audit data, 3-22 to 3-24
- entitlement reports
 - See reports, default entitlement

- EPHI Related Data Access Report, 3-13
- event activity summary, 2-37
- event categories
 - See audit events
- event handlers
 - fine-grained auditing, 2-13
 - relevant columns, 2-13
- EVENT_DIM dimension table
 - about, 4-4
 - contents of, 4-14
- exception events
 - Exception Activity Report, 3-8
 - IBM DB2, D-6
 - Oracle Database, A-10
 - SQL Server, B-9
 - Sybase Adaptive Server Enterprise, C-7

F

- fact tables
 - See data warehouse schema
- filtering data in reports, 3-26
- financial compliance reports
 - Financial Related Data Access Report, 3-12
 - Financial Related Data Modifications Report, 3-13
- financial data reports
 - See reports, compliance
- Financial Related Data Access Report, 3-12
- Financial Related Data Modifications Report, 3-13
- fine-grained auditing, 2-12
 - about, 2-12
 - audit policy, defining, 2-14
 - event handlers, 2-13
 - relevant columns, 2-13
- formatting reports, 3-16
- functions
 - in advanced alerts, 2-35

G

- general tasks for auditors using Oracle Audit Vault, 1-2

H

- health care compliance report
 - EPHI Related Data Access Report, 3-13
- health care reports
 - See reports, compliance
- hiding columns in reports, 3-24
- highlighting data in reports, 3-30

I

- IBM DB2
 - audit events
 - about, D-1
 - listed, D-1 to D-17
 - requirements for audit data collection, 1-6
- invalid record events

IBM DB2, D-7
Invalid Audit Record Report, 3-8
Oracle Database, A-11
SQL Server, B-11
Sybase Adaptive Server Enterprise, C-8

J

join operations
 filtering row data, 3-26

L

labels
 about, 3-19
 assigning snapshot to a label, 3-21
 comparing label data, 3-23
 creating label, 3-20
 generating individual label data, 3-22
 retrieving entitlement audit data, 3-20
 viewing data, 3-22 to 3-24

M

management activity reports
 See reports, default management activity
master records
 pulling column from report, 3-32
Microsoft SQL Server
 See SQL Server
monitoring alerts, 2-36

N

null values
 sorting in reports, 3-30

O

object management events
 IBM DB2, D-8
 Object Management Report, 3-7
 Oracle Database, A-13
 SQL Server, B-13
 Sybase Adaptive Server Enterprise, C-9
Object Privileges by Source Report, 3-11
Object Privileges Report, 3-11
objects
 See schema object auditing
objects being audited
 Deleted Objects Report, 3-14
 information in TARGET_DIM dimension table, 4-4
 Object Privileges by Source Report, 3-11
 Object Privileges Report, 3-11
Oracle Audit Vault
 about, 1-1
 audited data, types of, 1-2
 general tasks for auditors, 1-2
 IBM DB2 database requirements, 1-6
 Oracle Database requirements, 1-4

SQL Server database requirements, 1-6
Sybase Adaptive Server Enterprise database requirements, 1-6
 See also data warehouse schema, reports
Oracle Database
 audit events
 about, A-1
 listed, A-1 to A-25
 audit settings
 recommended in the database, 1-5
 checking audit settings in source database, 1-4
 requirements for audit data collection, 1-4
 retrieving audit settings, 2-2
Oracle Database Vault
 Database Vault Report, 3-5
 events, A-9
 finding if installed, 3-5
 provisioning audit policies settings to database, 2-20

P

peer association events
 Distributed Database Report, 3-5
 IBM DB2, D-10
 Oracle Database, A-16
 SQL Server, B-16
 Sybase Adaptive Server Enterprise, C-11
policies
 See audit policies
privilege auditing
 about, 2-10
 defining audit policy, 2-11
 statement auditing, compared with, 2-10
 System Privileges by Source Report, 3-11
 System Privileges Report, 3-11
privilege events
 See role and privilege management events
Privileged Users by Source Report, 3-11
Privileged Users Report, 3-11
privileges
 Privileged Users by Source Report, 3-11
 Privileged Users Report, 3-11
PRIVILEGES_DIM dimension table
 about, 4-5
 contents of, 4-14
Procedure Executions Report, 3-5
Procedure Management Report, 3-7
procedures
 See SQL statement auditing
Program Changes Report, 3-14

R

redo log file auditing
 about, 2-17
 defining capture rule for audit policy, 2-17
redo logs
 accessing before and after values, 4-18
relevant columns

- about, 2-13
- event handlers, 2-13
- fine-grained auditing, used in, 2-13
- reports
 - about, 3-1
 - accessing, 3-1
 - annotating, 3-18
 - attesting to, 3-18
 - changing default contents of compliance reports, 3-29
 - checking data collection status, 1-8
 - columns
 - adding control break, 3-32
 - finding information about, 3-33
 - hiding current column, 3-24
 - hiding or showing, 3-25
 - compliance, 3-11 to 3-15
 - creating charts, 3-31
 - customizing data display, 3-24 to 3-33
 - data collected for, 3-1
 - filtering
 - all rows based on current column, 3-26
 - default contents of compliance reports, 3-29
 - rows in one or all columns, 3-27
 - using an expression, 3-28
 - finding information
 - audit records, 3-33
 - column descriptions, 3-33
 - formatting, 3-15 to 3-18
 - highlighting rows, 3-30
 - PDF generation, 3-15 to 3-18
 - resetting display values to defaults, 3-33
 - saving to CSV file, 3-36
 - scheduling, 3-15 to 3-18
 - sending to other users, 3-15 to 3-18
 - setting retention time, 3-15 to 3-18
 - sorting data
 - all columns, 3-30
 - current column, 3-30
 - specifying auditors to attest to, 3-15 to 3-18
 - who can access, 3-1
 - See also* reports, compliance; reports, entitlement; reports, default; reports, user-defined
- reports, compliance
 - about, 3-11
 - Audit Settings Changes Report, 3-13
 - Before/After Values Report, 3-13
 - changing default contents, 3-29
 - common reports, 3-13
 - Credit Card Related Data Access Report, 3-12
 - Database Failed Logins Report, 3-14
 - Database Login/Logoff Report, 3-14
 - Database Logoff Report, 3-14
 - Database Logon Report, 3-14
 - Database Startup/Shutdown Report, 3-14
 - Deleted Objects Report, 3-14
 - EPHI Related Data Access Report, 3-13
 - Financial Related Data Access Report, 3-12
 - Financial Related Data Modifications Report, 3-13
- Program Changes Report, 3-14
- Schema Changes Report, 3-14
- System Events Report, 3-14
- User Privilege Change Activity Report, 3-15
- reports, default
 - Access Reports, 3-3 to 3-6
 - alert reports, 3-15
 - All Alerts Report, 3-15
 - compliance reports, 3-11 to 3-15
 - Critical Alerts Report, 3-15
 - Warning Alerts Report, 3-15
- reports, default access
 - Activity Overview Report, 3-4
 - Data Access Report, 3-4
 - Database Vault Report, 3-5
 - Distributed Database Report, 3-5
 - Procedure Executions Report, 3-5
 - User Sessions Report, 3-5
- reports, default entitlement
 - about, 3-9
 - Database Roles by Source Report, 3-10
 - Database Roles Report, 3-10
 - general steps for using, 3-19
 - Object Privileges by Source Report, 3-11
 - Object Privileges Report, 3-11
 - Privileged Users by Source Report, 3-11
 - Privileged Users Report, 3-11
 - System Privileges by Source Report, 3-11
 - System Privileges Report, 3-11
 - User Accounts by Source Report, 3-10
 - User Accounts Report, 3-10
 - User Privileges by Source Report, 3-10
 - User Privileges Report, 3-10
 - User Profiles by Source Report, 3-10
 - User Profiles Report, 3-10
 - See also* entitlement report snapshots and labels, 3-19
- reports, default management activity
 - about, 3-6
 - Account Management Report, 3-6
 - Audit Commands Report, 3-6
 - Object Management Report, 3-7
 - Procedure Management Report, 3-7
 - Role and Privilege Management Report, 3-7
 - System Management Report, 3-8
- reports, default system exception, 3-8 to 3-9
 - about, 3-8
 - Exception Activity Report, 3-8
 - Invalid Audit Record Report, 3-8
 - Uncategorized Activity Report, 3-9
- reports, financial
 - EPHI Related Data Access Report, 3-13
 - Financial Related Data Access Report, 3-12
 - Financial Related Data Modifications Report, 3-13
- reports, user-defined
 - accessing, 3-35
 - creating, 3-35
 - creating categories, 3-34
 - See also* reports

- respond to alerts, 2-38
- retention period for audit data, 2-39
- retention period for reports, 3-16
- role and privilege management events
 - IBM DB2, D-10
 - information in PRIVILEGE_DIM dimension table, 4-5
 - Oracle Database, A-17
 - Role and Privilege Management Report, 3-7
 - SQL Server, B-17
 - Sybase Adaptive Server Enterprise, C-12

S

- Sarbanes-Oxley Act
 - privilege auditing to meet compliance, 2-10
 - See also* compliance reports
- saving a report to CSV file, 3-36
- Schema Changes Report, 3-14
- schema object auditing
 - about, 2-8
 - defining audit policy, 2-8
 - Deleted Objects Report, 3-14
 - Object Privileges by Source Report, 3-11
 - Object Privileges Report, 3-11
- service and application utilization events
 - IBM DB2, D-12
 - Oracle Database, A-18
 - Procedure Executions Report, 3-5
 - SQL Server, B-20
 - Sybase Adaptive Server Enterprise, C-13
- session events
 - See* user session
- showing columns in reports, 3-24
- snapshots
 - about, 3-19
 - assigning snapshots to a label, 3-21
 - comparing snapshot data, 3-23
 - generating individual snapshot data, 3-22
 - retrieving entitlement audit data, 3-20
 - viewing data, 3-22 to 3-24
- sorting data in reports, 3-29
- SOURCE_DIM dimension table
 - about, 4-5
 - contents of, 4-15
- SQL script, saving the audit policy settings to, 2-20
- SQL Server
 - audit events
 - about, B-1
 - listed, B-1 to B-28
 - requirements for audit data collection, 1-6
- SQL statement auditing
 - about, 2-5
 - defining audit policy, 2-6
 - privilege auditing, compared with, 2-10
 - Procedure Executions Report, 3-5
 - Procedure Management Report, 3-7
- starting Audit Vault Console, 1-6
- statements
 - See* SQL statement auditing

- subqueries
 - filtering row data, 3-26
- Sybase Adaptive Server Enterprise
 - audit events
 - about, C-1
 - listed, C-1 to C-19
 - requirements for audit data collection, 1-6
- system audit events
 - System Events Report, 3-14
- System Events Report, 3-14
- system exception reports
 - See* reports, default system exception
- system management events
 - IBM DB2, D-13
 - Oracle Database, A-20
 - SQL Server, B-21
 - Sybase Adaptive Server Enterprise, C-15
 - System Management Report, 3-8
- System Privileges by Source Report, 3-11
- System Privileges Report, 3-11

T

- TARGET_DIM dimension table
 - about, 4-4
 - contents of, 4-15
- time, actions performed over
 - information in TIME_DIM dimension table, 4-4
- TIME_DIM dimension table
 - about, 4-4
 - contents of, 4-16
- trouble ticket notifications
 - creating, 2-38
- trouble tickets
 - creating a notification, 2-38
 - creating a template for, 2-26
- troubleshooting
 - database auditing not enabled, 1-4
 - Database Vault report not showing data, 3-5
 - latest audit data not appearing in reports, 3-4
 - no data in reports, 1-8
 - source database not available, 1-8

U

- Uncategorized Activity Report, 3-9
- unknown or uncategorized events
 - IBM DB2, D-15
 - Oracle Database, A-22
 - SQL Server, B-24
 - Sybase Adaptive Server Enterprise, C-17
 - Uncategorized Activity Report, 3-9
- User Accounts by Source Report, 3-10
- User Accounts Report, 3-10
- user login failure audit events
 - Database Failed Logins Report, 3-14
- User Privilege Change Activity Report, 3-15
- User Privileges by Source Report, 3-10
- User Privileges Report, 3-10
- User Profiles by Source Report, 3-10

- User Profiles Report, 3-10
- user session events
 - IBM DB2, D-16
 - Oracle Database, A-23
 - SQL Server, B-26
 - Sybase Adaptive Server Enterprise, C-18
 - User Sessions Report, 3-5
- User Sessions Report, 3-5
- USER_DIM dimension table
 - about, 4-4
 - contents of, 4-18
- user-defined reports
 - accessing, 3-35
 - creating, 3-35
 - creating categories, 3-34
 - deleting, 3-35
- users
 - Database Roles Report, 3-10
 - information in USER_DIM dimension table, 4-4
 - logging in to the Audit Vault Console, 1-6
 - login and logoff operations, Database
 - Login/Logoff Report, 3-14
 - logoff operations, report, 3-14
 - Privileged Users by Source Report, 3-11
 - Privileged Users Report, 3-11
 - User Accounts Report, 3-10
 - User Privilege Change Activity Report, 3-15
 - User Privileges by Source Report, 3-10
 - User Privileges Report, 3-10
 - User Profiles by Source Report, 3-10
 - User Profiles Report, 3-10

W

- Warning Alerts Report, 3-15
- Windows Event Viewer
 - audit events logged in, B-6
 - exception events logged in, B-9

