Oracle® Audit Vault and Database Firewall

Auditor's Guide

Release 12.1.2

E27777-15

July 2017

ORACLE®

Oracle Audit Vault and Database Firewall Auditor's Guide, Release 12.1.2

E27777-15

Primary Author: Gigi Hanna

Contributing Authors: Maitreyee Chaliha, Tanmay Choudhury, Pat Huey, Sheila Moore

Contents

2 Managing Secured Targets

3 Managing Access and Other Settings

4 Creating Database Firewall Policies

5 Creating Audit Policies for Oracle Databases

6 Generating Reports

7 Managing Entitlements

8 Creating Alerts

A Oracle Audit Vault and Database Firewall Database Schemas

B Audit Record Fields

C Oracle Database Audit Events

D Sybase ASE Audit Events

E Microsoft SQL Server SQL Trace Audit Events

F Microsoft SQL Server SQL Audit and Event Log Events

G IBM DB2 Audit Events

H MySQL Audit Events

I Solaris Operating System Audit Events

J Microsoft Windows Operating System Audit Events

K Linux Operating System Audit Events

L Oracle ACFS Audit Events

M Active Directory Audit Events

Index

List of Figures

List of Tables

Preface

Oracle Audit Vault and Database Firewall Auditor's Guide explains how an auditor uses Oracle Audit Vault and Database Firewall (referred to as Oracle AVDF).

This preface contains the following topics:

Audience

This document is intended for security managers, audit managers, and database administrators (DBAs) who are involved in the configuration of Oracle Audit Vault and Database Firewall.

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 that have purchased support 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, see the following documents in the Oracle Other Product One Release 7.0 documentation set or in the Oracle Other Product Two Release 6.1 documentation set:

- *Oracle Audit Vault and Database Firewall Release Notes*
- *Oracle Audit Vault and Database Firewall Administrator's Guide*
- *Oracle Audit Vault and Database Firewall Installation Guide*
- *Oracle Audit Vault and Database Firewall Developer's Guide*

Conventions

The following text conventions are used in this document:

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

Quick Reference for Common Tasks

Topics

About this Quick Reference

This chapter is intended for users familiar with Oracle Audit Vault and Database Firewall (AVDF), and who want to quickly locate step-by-step instructions for common tasks. If you are new to Oracle AVDF, we recommend you first read the introductory material to get an understanding of the system.

Secured Targets

User Accounts and Access Rights

Email Notifications

Status and Job Monitoring

Firewall Policies

Creating, Copying, and Editing Firewall Policies

Defining a Firewall Policy

Publishing and Deploying a Firewall Policy

Audit Policies (for Oracle Databases)

Retrieving Existing Audit Policies from the Database

Creating New Audit Policies

Provisioning Audit Policies to the Database

Reports

Entitlements

Alerts

1

Introducing Oracle Audit Vault and Database Firewall

Topics

Downloading the Latest Version of This Manual

You can download the latest version of this manual from the following website:

`http://www.oracle.com/pls/topic/lookup?ctx=avdf121`

You can find documentation for other Oracle products at the following website:

`http://docs.oracle.com`

System Features

Topics

About Oracle Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall (AVDF) secures databases and supported operating systems in two ways:

- For databases, it provides a database firewall that can monitor and/or block SQL statements based on a firewall policy designed by an auditor, and provides a set of firewall reports.
- For databases and supported operating systems, it collects audit data, and makes it available in audit reports. For Oracle databases, Oracle AVDF lets an auditor set audit policies and provision them from the Audit Vault Server console.

Supported Secured Targets

A secured target is any database or other target type (such as an operating system) that you are monitoring and securing with Oracle AVDF. The secured target types supported out-of-the-box are:

- Oracle Database
- IBM DB2 for LUW
- Microsoft SQL Server
- MySQL
- SQL Anywhere
- Sybase
- Solaris Operating System
- Oracle ACSF
- Windows Operating System
- Windows Active Directory
- Linux Operating System

See *Oracle Audit Vault and Database Firewall Administrator's Guide* for the specific Oracle AVDF features supported for each secured target type and version.

Other types of secured targets can be monitored by deploying custom plug-ins, available from Oracle or third parties. Oracle also provides the *Oracle Audit Vault and Database Firewall Developer's Guide* to create your own custom plug-ins.

Additional Platform Information

See *Oracle Audit Vault and Database Firewall Installation Guide* for detailed platform support for the current release.

In addition, you can find platform information for prior releases in **Article 1536380.1** at the following website:

`https://support.oracle.com`

Auditing Features

Oracle AVDF auditing features allow an auditor to configure and manage the following:

- Firewall policies
- Audit policies for Oracle Database

- Reports and report schedules
- Fetching entitlement audit data for Oracle Database
- Stored procedure auditing
- Alerts and email notifications
- Access rights to secured targets and groups (super auditors only)

Administrative Features

Oracle AVDF administrative features allow an administrator to configure and manage the following:

- Secured Targets, their host computers, and their audit trail collection
- Audit Vault Agent deployment
- Database Firewalls in the database network
- Audit data lifecycle, archiving, and purging
- High Availability
- Third party integrations
- Access rights to secured targets and groups (super administrators only)

See *Oracle Audit Vault and Database Firewall Administrator's Guide* for detailed information on administrative functions.

Integrations With Third-Party Products

You can integrate Oracle AVDF with the following third-party products:

- **BIG-IP Application Security Manager (ASM):** This product from F5 Networks, Inc. is an advanced Web Application Firewall (WAF) that provides comprehensive edge-of-network protection against a wide range of Web-based attacks. It analyzes each HTTP and HTTPS request, and blocks potential attacks before they reach the Web application server.
- **ArcSight Security Information Event Management (SIEM):** This product is a centralized system for logging, analyzing, and managing syslog messages from different sources.

See the *Oracle Audit Vault and Database Firewall Administrator's Guide* for information on configuring these integrations.

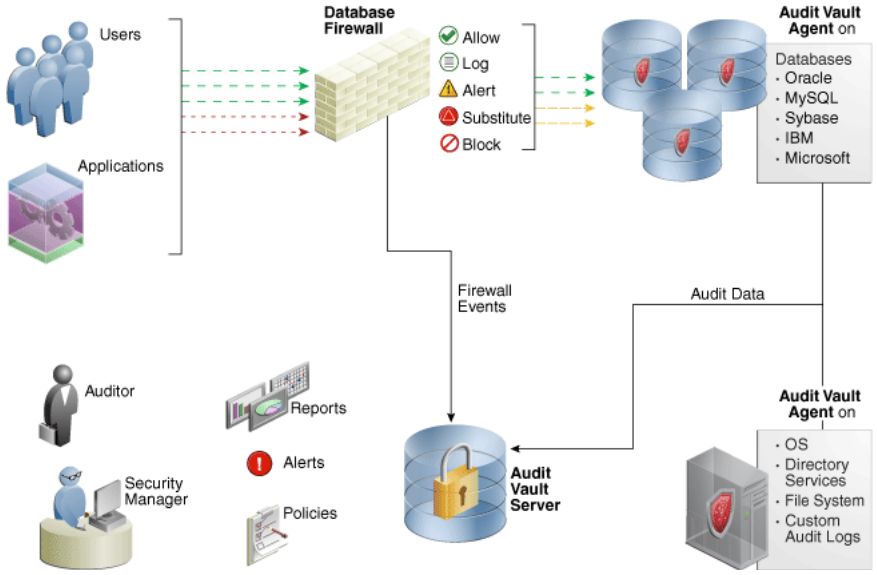
Component Architecture

Topics

How Oracle AVDF Components Work Together

Oracle AVDF includes the Audit Vault Server, the Database Firewall, and the Audit Vault Agent. Figure 1–1 provides a high-level overview of how these components work together.

Figure 1–1 Audit Vault and Database Firewall Architecture



The process flow for the Oracle AVDF components is as follows:

1. For each secured target, the Audit Vault Agent has been deployed, and/or the Database Firewall has been placed in the network and configured to protect that target.

   If the agent has been deployed, Oracle AVDF is configured to collect the appropriate audit trail from the secured target. If the Database Firewall is protecting the target, a firewall policy has been applied for that target.

   You can configure multiple secured targets from different database product families, as well as non-database products, using the same Audit Vault Server.

2. The Audit Vault Agent retrieves the audit data from secured targets and sends this data to the Audit Vault Server.

   The Database Firewall monitors SQL traffic to database secured targets and sends that data to the Audit Vault Server. The firewall can be configured to monitor and raise alerts only, or to block SQL traffic and optionally substitute statements according to a policy.

3. The Audit Vault Server collects and stores data from the Audit Vault Agent and Database Firewall in its internal data warehouse.

   The data warehouse organizes this data into a set of internal dimension tables. The Audit Vault Server stores other information as well, for both the auditor and the administrator.

4. Once the audit data is in the data warehouse dimension tables, an auditor can generate and customize reports, as well as configure email notifications.

   Any settings that you create, such as security settings, are contained in this server.

The Audit Vault Server

The Audit Vault Server contains the tools necessary to configure Oracle AVDF to collect audit data from, and apply firewall policies to, your secured targets. The Audit Vault Server also contains an Oracle database, and makes it available to reporting tools through a data warehouse.

The Audit Vault Server provides the following services:

- Audit data collection and lifecycle management
- Audit Vault Agent management
- Database Firewall management
- Audit and firewall policy management
- Reporting
- Alerting and notification management
- User entitlement auditing
- Stored Procedure Auditing
- Archive and backup
- High availability mode
- Published data warehouse that can be used with reporting tools such as Oracle Business Intelligence Publisher to create customized reports
- User access management
- Third party integrations

The Database Firewall

The Database Firewall is a dedicated server that runs the Database Firewall software. Each Database Firewall collects SQL data from secured target databases, and then sends the data to the Audit Vault Server to be analyzed in reports.

An Oracle AVDF auditor can create firewall policies that define rules for how the Database Firewall handles SQL traffic to the database secured target. The firewall policy specifies the types of alerts to be raised in response to specific types of SQL statements, and when to block or substitute harmless SQL statements for potentially harmful statements. To do this, the Database Firewall can operate in one of two modes:

- **DPE Mode:** Database Policy Enforcement. When in this mode, the Database Firewall applies rules in a firewall policy to monitor SQL traffic to your secured target database and block traffic, and/or substitute benign SQL statements for potentially destructive ones.
- **DAM Mode:** Database Activity Monitoring. When in this mode, the Database Firewall applies rules in a firewall policy to monitor and raise alerts about potentially harmful SQL traffic to your secured target database, but it does not block or substitute SQL statements.

In order to control how the Database Firewall protects a database secured target, the administrator configures enforcement points for each secured target. The enforcement point specifies whether the firewall operates in DPE or DAM mode, which firewall policy to apply to the secured target, and other settings.

The Audit Vault Agent

The Agent retrieves the audit trail data from a secured target database and sends it to the Audit Vault Server. The Agent sends both valid and invalid audit records, gets configuration information, and sends error records using Oracle Call Interface (OCI) and JDBC password-based authentication. If the Agent is stopped, then the secured target database will still create an audit trail (assuming auditing is enabled). The next time you restart the Agent, then Oracle AVDF retrieves the audit data that had been accumulating since the Agent was stopped.

The Audit Vault Agent also contains host monitoring software that monitors SQL traffic to a database over the network and sends this information to a Database Firewall. For detailed information on host monitoring, see *Oracle Audit Vault and Database Firewall Administrator's Guide*.

The Oracle AVDF administrator configures one Audit Vault Agent for each host and one or more audit trails for each individual secured target database. See the *Oracle Audit Vault and Database Firewall Administrator's Guide* for information on all administration functions.

The Auditor's Role

As an auditor, you use the Audit Vault Server console to configure the following for databases or non-databases you are monitoring with Oracle AVDF:

- **Secured Targets** - For each target you are monitoring, the Oracle AVDF administrator must configure a secured target in the Audit Vault Server. As an auditor, you can then specify audit and/or firewall policies for the secured target, as well as other requirements. See "Understanding Secured Targets" on page 1-7.
- **Firewall Policies** - For any supported database, you can use the Database Firewall and design a firewall policy based on analyzed SQL statements from your secured targets. See "Creating Database Firewall Policies" on page 4-1 for details.
- **Audit Policies** - For Oracle databases, you can use Oracle AVDF to design audit policies and provision them to the database. See "Creating Audit Policies for Oracle Databases" on page 5-1 for details.
- **Alerts and Notifications** - You can create simple or complex alerts based on conditions you specify for the secured targets you are monitoring. You can also specify alert notifications using email templates. See "Creating Alerts" on page 8-1 for details.
- **Audit Trails** - For any secured target type, you can monitor the status of audit trails and see audit reports. See "Viewing a List of Audit Trails" on page 2-2.
- **Reports** - You can schedule and generate a variety of audit and firewall reports in Oracle AVDF, create report notifications, as well as add your own customized reports. See "Generating Reports" on page 6-1 for details.

Auditor Roles in Oracle AVDF

There are two auditor roles in Oracle AVDF, with different access levels:

- **Super Auditor** - This role has access to all secured targets and can grant access to specific secured targets and groups to an auditor. A super auditor can also assign the super auditor role to others.
- **Auditor** - This role can only see data for secured targets to which they have been granted access by a super auditor.

See "Managing Access and Other Settings" on page 3-1.

Understanding Secured Targets

A secured target is any supported database or non-database that you monitor with Oracle AVDF. Secured targets can be monitored by the Audit Vault Agent, the Database Firewall, or both.

The Oracle AVDF administrator creates and configures secured targets, providing host addresses, usernames, passwords, and other necessary information.

If a secured target is monitored by a Database Firewall, the Oracle AVDF administrator configures the Database Firewall, and also configures an enforcement point for each secured target.

Once secured targets are configured, an auditor can do the following for each one:

- Collect audit data
- Enable stored procedure auditing (SPA)
- If the target is a database secured by a Database Firewall:
  - Design and apply a firewall policy
  - View the status of configured enforcement points
- If the secured target is an Oracle database:
  - Define and provision the audit policies
  - Retrieve user entitlement information
- Set a data retention policy
- Generate a variety of reports
- Monitor audit trail status

Super auditors can create secured target groups for access control purposes. Super auditors grant auditors access to individual secured targets or to target groups.

For details on secured targets, see "Managing Secured Targets" on page 2-1.

Understanding Firewall Policies

Oracle AVDF lets you protect database secured targets with a database firewall. The firewall monitors SQL traffic to the database, logs activity, sends alerts, and can also block specific types of SQL statements and replace them with substitute statements that you configure.

A firewall policy determines how the database firewall handles SQL traffic to the secured target database. Oracle AVDF includes a firewall policy editor that lets you design a firewall policy. You can design the policy by analyzing your current SQL statement traffic, and then configuring settings in the firewall policy based on these statements.

Once you design the policy in the Audit Vault Server policy editor, you can upload it to a secured target in the auditor console. You can assign a different policy to different secured targets.

For details, see "Creating Database Firewall Policies" on page 4-1.

Planning the Protection Level for Your Databases

Depending on operational needs, Database Firewall can operate in one of the following modes:

- **Database Activity Monitoring (DAM):** The system detects and logs unusual activity, and produces warnings, but does not block potential threats. This is useful during the early stages of deployment while you are developing and refining a policy. It is also known as monitoring mode.
- **Database Policy Enforcement (DPE):** The system performs all the actions of database activity monitoring and blocks potential attacks. It is also known as blocking mode.

These modes operate independently. For example, one Database Firewall can simultaneously monitor one secured target while blocking another.

Consider what you want the Database Firewall to achieve for you. Do you want:

- Access logging?
- Warnings of potential attacks?
- Blocking of potential attacks?

In general, implementing only audit logging requires the least up-front development time to create a satisfactory policy. SQL statement blocking requires the most development time, but provides the greatest protection.

One strategy for deployment is to start with audit logging only, and then deploy a policy file that can protect the database against potential attacks at a later date. This helps you to become familiar with the deployment.

If you want to block SQL statements eventually, then using Database Activity Monitoring (DAM) can build confidence before you deploy the system fully.

When DAM mode is set, policies can include block action levels, *but* statements with specified action levels pass straight through. Syslog events and reports show the statements as blocked, while in reality, the statements passed through normally. This enables you to evaluate the system in a live environment before you switch on statement blocking. During this evaluation phase, you can change the policy to modify the system responses.

Understanding Audit Policies and Audit Data Collection

Topics

About Audit Policies and Audit Data Collection

The Oracle AVDF administrator configures Oracle Database and other types of secured targets (both databases and non-databases). As an auditor, you can then retrieve audit data from these secured targets and generate various reports.

If the secured target is an Oracle Database, Oracle AVDF also lets you configure and provision audit policies for that database. You can then retrieve the current audit settings from an Oracle Database and modify them, as well as add new audit policies, for the following:

- SQL statements
- Database objects
- Fine-grained auditing
- Capture rules for redo log activity

Once you have configured the audit policies for an Oracle Database, you can then provision them to the database. You will then be able to see, in the Audit Vault Server console, if those policies are changed by a database administrator at the database.

For details, see "Creating Audit Policies for Oracle Databases" on page 5-1.

Requirements for Collecting Audit Data from Secured Targets

Topics

Requirements for Oracle Database

Topics

Ensuring That Auditing Is Enabled in the Secured Target Database Before Oracle AVDF can collect audit data from the secured target 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.

Using Recommended Audit Settings in the Secured Target 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;`

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 databases and *Oracle Audit Vault and Database Firewall Administrator's Guide*.

Configuring Alerts and Notifications

Oracle AVDF lets you define rule-based alerts on audit records and specify notification actions for those alerts. Whenever an audit event meets the rule or condition defined in the alert definition, an alert is raised and a notification is sent as specified. You can define alerts by type of secured target, the number of times an event occurs, and by using available fields in audit records to define a Boolean condition that must be met. You can also configure email templates to be used for alert notifications.

You can monitor and respond to alerts from the Audit Vault Server console and from alert reports.

For details, see "Creating Alerts" on page 8-1.

Generating Reports

As an Oracle AVDF auditor, you can generate various audit reports for the secured targets to which you have access. You can schedule, print, and/or email the reports to others, in PDF or XLS format. Reports include information on audit data, entitlements, and stored procedures. You can also generate compliance reports to meet regulations associated with credit card, financial, data protection, and health care-related data.

Oracle AVDF also lets you browse and customize report data interactively, and upload your own custom reports created with third party tools.

For details, see:

- "Generating Reports" on page 6-1
- "Managing Entitlements" on page 7-1

Creating Users and Managing Access

A super auditor creates auditor accounts, and manages auditor access to secured targets and secured target groups. For information on these functions, see "Managing Access and Other Settings" on page 3-1.

Logging in to Audit Vault Server Console

Topics

Logging in to the Audit Vault Server Console

To log in to the Audit Vault Server console:

1. From a browser, enter the following URL:

   `https://host/console`

   where *host* is the server where you installed Audit Vault Server.

   For example:

   `https://192.0.2.1/console`

2. In the Login page, enter your user name and password, and then click **Login**.

   The **Home** page appears.

Understanding the Tabs in the Audit Vault Server Console UI

When you log into Audit Vault Server console as an auditor or super auditor, you see the auditor's dashboard on the Home page, and the functions available for the auditor roles.

From the Home tab, you can:

- Select a date range for viewing event data.

- 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:
  - **Recently Raised Alerts**

    This area displays alerts raised within the period you selected. You can view specific alert levels by clicking **See all Warning Alerts** or **See All Critical Alerts**.
  - **Attestation Actions**

    See report attestation actions you need to take within your selected time range.
  - **Top Five Audit Sources by Number of Alerts**

    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.
  - **Failed Logins**

    See failed logins within your selected time range.

Other tabs let you access the following functions:

- **Secured Targets** - lets you set firewall, audit, and data retention policies for each secured target, manage entitlement snapshots, set up secured target groups, see audit trails and enforcement points
- **Reports** - lets you generate default reports, schedule reports, customize reports online, and upload your custom reports
- **Policy** - lets you manage audit and firewall policies, and configure alerts
- **Settings** - lets you change your password, create and manage email distribution lists, configure email notification templates for alerts and reports, view audit trail and enforcement point status, manage user accounts and access, and view job status.

The following Quick Links are available from all tabs:

- **Enforcement Points** - lets you check enforcement point details and status
- **Audit Trails** - lets you check audit trail details and status

Working with Lists of Objects in the UI

Throughout the Audit Vault Server UI, you will see lists of objects such as reports, users, secured targets, firewall policies, etc. You can filter and customize any of these lists of objects in the same way as you can for Oracle AVDF reports. This section provides a summary of how you can filter and custom the display of lists of objects. For more detailed information, see the "Filtering and Controlling the Display of Data in a Report" on page 6-3.

To filter and control the display of lists of objects in the Audit Vault Server UI:

1. To find an item in the list, enter its name in the search box, and then click **Go**.
2. To customize the list, from the **Actions** menu, select any of the following:
   - **Rows Per Page:** Select the number of rows to display per page.
   - **Select Columns:** Select which columns to display.

- **Filter:** Filter the list by column or by row using regular expressions with the available operators. When done, click **Apply**.
- **Format:** Format the list by selecting from the following options:
  - **Sort**
  - **Control Break**
  - **Highlight**
  - **Chart**
  - **Group By**

  Fill in the criteria for each option as needed and click **Apply**.
- **Save Report:** Save the current view of the list. Enter a name and description and click **Apply**.
- **Reset:** Reset the list to the default view.
- **Download:** Download the list. Select the download format (CSV or HTML) and click **Apply**.

2

Managing Secured Targets

Topics

About Managing Secured Targets

Secured targets are created by an Oracle AVDF administrator. A secured target is created for each database or other supported audit source for which you want to retrieve audit data, and/or for a database you want to monitor with a database firewall.

As an auditor, you can view data for secured targets to which a super auditor has granted you access.

You can use the **Secured Targets** tab of the Audit Vault Server console to control the following aspects of the secured targets that you can access:

- View and sort the list of secured targets. See "Working with Lists of Objects in the UI" on page 1-12.
- View, change, or access the following for each secured target:
  - Audit trails
  - Enforcement points
  - Firewall policy
  - Audit policy (for Oracle databases only)
  - User entitlements (for Oracle databases only)
  - Stored Procedure Auditing (SPA)
  - Retention policy
- Create or modify secured target groups
- Manage entitlement snapshots and labels

Viewing and Changing Settings for a Secured Target

Topics

Viewing a List of Audit Trails

An Oracle AVDF administrator starts and stops audit trails. As an auditor, you can view lists of audit trails for secured targets you have access to. You can see the trails collected for a single secured target or for all your secured targets:

Viewing a List of Audit Trails for One Secured Target

To view audit trails for a secured target:

1. Log into the Audit Vault Server console as an auditor, and click the **Secured Targets** tab.
2. Select a secured target from the list.

   You can adjust the appearance of the list from the **Actions** menu. See "Working with Lists of Objects in the UI" on page 1-12.
3. Click the arrow to expand the **Audit Trails** section in this secured target.

   Audit trails for this secured target are listed in a table showing the trail, its status, its trail type, and the host from which the trail was collected.
4. Optionally, click the up or down arrow in a column title to sort (ascending or descending) by that column.

Viewing a List of Audit Trails for All Your Secured Targets

To view a list of audit trails for all your secured targets:

1. Log into the Audit Vault Server console as an auditor, and click the **Settings** tab or the **Secured Targets** tab.
2. From the **Quick Links** menu, click **Audit Trails**.

   Audit trails for all your secured targets are listed in a table showing the trail, its status, the secured target name and type, and the host from which the trail was collected, the trail location and type.

   You can adjust the appearance of the list from the **Actions** menu. See "Working with Lists of Objects in the UI" on page 1-12.
3. Optionally, click a column title to sort by that column.

Viewing a List of Enforcement Points

An Oracle AVDF administrator creates enforcement points for database secured targets monitored by a database firewall. As an auditor, you can see the enforcement points configured for the database secured targets you have access to. You can see the enforcement points for one secured target or for all your secured targets:

- Viewing a List of Enforcement Points for One Database Secured Target
- Viewing a List of Enforcement Points for All Your Secured Target Databases

Viewing a List of Enforcement Points for One Database Secured Target

To list the enforcement points for a database secured target:

1. Log into the Audit Vault Server console as an auditor, and click the **Secured Targets** tab.
2. From the Secured Targets list, select a secured target.
3. Click the arrow to expand the **Enforcement Points** section in this secured target. This section is not visible if the secured target is not a database.
4. Click the name of the enforcement point to see its details.

Viewing a List of Enforcement Points for All Your Secured Target Databases

To list enforcement points configured for all your database secured targets:

1. Log into the Audit Vault Server console as an auditor, and click the **Settings** tab or the **Secured Targets** tab.
2. From the **Quick Links** menu, click **Enforcement Points**.
3. Click the name of the enforcement point to see its details.

Selecting a Firewall Policy

If a secured target is a database monitored by a Database Firewall, you can upload or change the firewall policy assigned to the secured target.

To set or change the firewall policy for a database secured target:

1. Log into the Audit Vault Server console as an auditor, and click the **Secured Targets** tab.
2. Select a secured target from the list.
3. Click the arrow to expand the **Firewall Policy** section in this secured target.

   The firewall policy set for this secured target is listed.

   (The **Firewall Policy** section is not visible if the secured target is not a database.)
4. To change the firewall policy, click **Change**, select a different policy from the drop-down list, and then click **Save**.

   The drop-down list contains preloaded firewall policies as well as those created by auditors.

For detailed information on firewall policies, see "Creating Database Firewall Policies" on page 4-1.

Viewing Audit Policy Settings for Oracle Databases

You can view audit policy settings for Oracle databases from the Secured Targets tab.

To view audit settings for Oracle databases from the secured target page:

1. Log into the Audit Vault Server console as an auditor, and click the **Secured Targets** tab.
2. Select a secured target from the list.
3. Click the arrow to expand the **Audit Policy** section in this secured target. If the secured target is not an Oracle database you will not see an Audit Policy section.

   The **Retrieve Audit Settings** button allows you to retrieve this Oracle Database's audit settings at this point in time. See "Retrieving Audit Settings from an Oracle Database" on page 5-2.

   Audit policies for this secured target are listed in a table showing audit type, number of settings in use and the number needed, and the number of problems flagged. You can click the link for each audit type to go to the Audit Settings page (**Policy** tab), and from there, modify the settings. See "Specifying Which Audit Settings Are Needed" on page 5-3.

For detailed information on audit policies, see "Creating Audit Policies for Oracle Databases" on page 5-1.

Retrieving User Entitlement Data for Oracle Database Secured Targets

When you retrieve user entitlement data for an Oracle Database secured target, a snapshot of the data at this point in time is added to the entitlement snapshots retrieved at earlier points in time. From there, you can organize snapshots by assigning them labels, and compare entitlement data from different snapshots or labels. See "Working With Entitlement Snapshots and Labels" on page 7-2.

To retrieve entitlement data for a secured target:

1. Log into the Audit Vault Server console as an auditor, and click the **Secured Targets** tab.
2. Select a secured target from the list.
3. Click the arrow to expand the **User Entitlements** section in this secured target.

   The timestamp of when entitlement data was last retrieved, if any, appears.
4. Click **Retrieve User Entitlement Data**.

   A confirmation message appears.

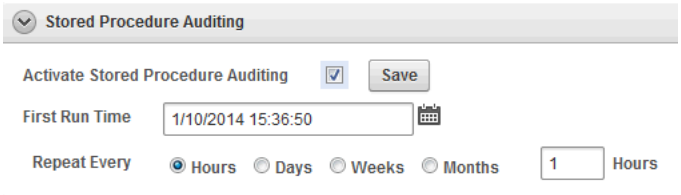
You can check the status of entitlement retrieval by clicking **Jobs** in the **Settings** tab.

Activating Stored Procedure Auditing

You can audit changes to stored procedures in a secured target in Oracle AVDF reports (see "Stored Procedure Auditing Reports" on page 6-18). In order to see this data for a database secured target, you must activate Stored Procedure Auditing for that secured target.

To activate stored procedure auditing for a secured target:

1. Log in to the Audit Vault Server console as an auditor.
2. Click the **Secured Targets** tab, and then click the name of the secured target you want.
3. Scroll down and expand the Stored Procedure Auditing section.
4. Select **Activate Stored Procedure Auditing**.



5. Set the following fields:
   - **First Run Time:** Select the date and time to run stored procedure auditing for this database for the first time.
   - **Repeat Every:** Select how often to repeat stored procedure auditing for this database.
6. Click **Save**.

Note: In order to collect stored procedure changes from a secured target database, your Oracle AVDF administrator must run scripts to set up the correct user privileges on that database. See *Oracle Audit Vault and Database Firewall Administrator's Guide* for information.

Setting a Data Retention (Archiving) Policy

The data retention policy for a secured target determines how long audit data is retained for that target. An Oracle AVDF administrator creates retention policies, and an auditor selects one of the available policies to assign to a secured target.

If you do not select a retention policy for a secured target, the default retention policy will be used (12 months retention online and 12 months in archives before purging).

A new retention policy takes effect as of the date you select the policy, but does not apply to existing data.

To set a data retention policy for a secured target:

1. Log into the Audit Vault Server console as an auditor, and click the **Secured Targets** tab.
2. Select a secured target from the list.
3. Click the arrow to expand the **Retention Policy** section in this secured target.

   The current retention policy, if set, is listed.
4. To set or change the retention policy, click **Change**, and then select from the available retention policies.
5. Click **Save**.

For information on configuring retention (archiving) policies, see the *Oracle Audit Vault and Database Firewall Administrator's Guide*.

Creating and Modifying Secured Target Groups

Topics

About Secured Target Groups

As a super auditor you can organize secured targets into groups for the purpose of granting auditor access to them as a group instead of individually.

Oracle AVDF provides a set of preconfigured user groups related to compliance categories, for example HIPAA or DPA. You can add secured targets to those groups to generate the specific compliance reports related to those databases.

Creating and Modifying Secured Target Groups

As a super auditor you can create secured target groups in order to grant other administrators access to secured targets as a group rather than individually.

To create a secured target group:

1. Log into the Audit Vault Server console as an auditor, and click the **Secured Targets** tab.
2. From the **Manage** menu on the left, click **Groups**.

   Preconfigured groups are listed in the bottom pane, and user-defined groups are listed in the top pane.

   You can adjust the appearance of the list in the bottom pane from the **Actions** menu. See "Working with Lists of Objects in the UI" on page 1-12.
3. Click **Create**, and enter a name and optional description for the group.
4. To add secured targets to the group, select the secured targets, and click **Add Members**.
5. Click **Save**.

   The new group appears in the top pane of the groups page.

To modify a secured target group:

1. Log into the Audit Vault Server console as an auditor, and click the **Secured Targets** tab.
2. From the **Manage** menu on the left, click **Groups**.

   Preconfigured groups are listed in the bottom pane, and user-defined groups are listed in the top pane.

   You can adjust the appearance of the list in the bottom pane from the **Actions** menu. See "Working with Lists of Objects in the UI" on page 1-12.
3. Click the group name.
4. In the Modify Secured Target Group page, select secured targets you want to add or remove, and then click **Add Members** or **Drop Members**.
5. Optionally, you can change the name or description of a user-defined group.
6. Click **Save**.

Managing Compliance for Secured Target Databases

To ensure that the correct compliance reports are available for secured target databases, you add those secured targets to the appropriate preconfigured group in the Audit Vault Server. For more information on compliance reports, see "Compliance Report Descriptions" on page 6-18.

To assign a secured target to a compliance group:

1. Log into the Audit Vault Server console as an auditor, and click the **Secured Targets** tab.
2. From the **Manage** menu, click **Groups**.

   The groups page appears, listing user-defined groups and preconfigured secured target groups.
3. In the Preconfigured Secured Target Groups section, click a compliance group. For example, select HIPAA.
4. In the Modify Secured Target Group page, select the secured target databases to add to this compliance group, and then click **Add Members**.
5. To remove a secured target database from the compliance group, select the secured target, and then click **Drop Members**.
6. Click **Save**.

Setting Access Rights for Secured Targets and Groups

If you have the super auditor role in Oracle AVDF, you can set access rights for secured targets and groups. Only auditors that have been granted access to specific secured targets or groups will be able to see them or data related to them. You can manage access by secured target or group, or by user.

See "Managing User Accounts and Access" on page 3-1 for instructions.

3

Managing Access and Other Settings

Topics

Managing User Accounts and Access

Topics

About Oracle AVDF Auditor Accounts and Passwords

There are two types of auditor accounts in Oracle AVDF:

- **Super Auditor:**
  - Creates user accounts for super auditors and auditors
  - Has auditor access to all secured targets and secured target groups
  - Grants auditor access to secured targets or secured target groups to auditors
- **Auditor:** Has access to specific secured targets or secured target groups granted by a super auditor

Passwords for these accounts need not be unique; however, Oracle recommends that passwords:

- Have at least one uppercase alphabetic, one alphabetic, one numeric, and one special character (plus sign, comma, period, or underscore).
- Be between 8 and 30 characters long.
- Be composed of the following characters:

  - Lowercase letters: a-z.
  - Uppercase letters: A-Z.
  - Digits: 0-9.
  - Punctuation marks: comma (,), period (.), plus sign (+), colon(:), and underscore (_).
- Not be the same as the user name.
- Not be an Oracle reserved word.
- Not be an obvious word (such as welcome, account, database, and user).
- Not contain any repeating characters.

Creating Auditor Accounts in Oracle AVDF

Super auditors can create both super auditor and auditor user accounts.

To create an auditor account in Oracle AVDF:

1. Log in to the Audit Vault Server console as a super auditor.
2. Click the **Settings** tab.

   The Manage Auditors page appears by default, and displays existing users and the secured targets and/or groups to which they have access.
3. Click **Create**.
4. Enter the **User Name** and **Password**, and re-type the password in the appropriate fields.

   Note that Oracle AVDF does not accept user names with quotation marks, such as "jsmith".
5. In the **Type** drop-down list, select **Auditor** or **Super Auditor**.

   See "About Oracle AVDF Auditor Accounts and Passwords" on page 3-1 for an explanation of these roles.
6. Click **Save**.

   The new user is listed in the Manage Auditors page.

Managing User Access to Secured Targets or Groups

Topics

About Managing User Access

Super auditors have access to all secured targets and secured target groups, and can grant access to specific targets and groups to auditors.

You can control access to secured targets or groups in two ways:

- Modify a secured target or group to grant or revoke access for one or more users.

- Modify a user account to grant or revoke access to one or more secured targets or groups.

Controlling Access by User

To control which secured targets or groups are accessible by a user:

1. Log in to the Audit Vault Server console as a super auditor.
2. Click the **Settings** tab, then click **Manage Auditors**.

   The Manage Auditors page displays existing users and the secured targets or groups to which they have access.
3. Click the name of the user account you want to modify.

   The Modify Auditor page appears.
4. In the Targets and Groups section, select the secured targets or secured target groups to which you want to grant or revoke access for this user.
5. Click **Grant Access** or **Revoke Access**.

   A check mark indicates access granted. An "x" indicates access revoked.
6. If necessary, repeat steps 4 and 5.
7. Click **Save**.

Controlling Access by Secured Target or Group

To control which users have access to a secured target or group:

1. Log in to the Audit Vault Server console as a super auditor.
2. Click the **Settings** tab, and then click **Manage Access**.
3. Click the name of the secured target or secured target group for which you want to define access rights.

   The Modify Access page for this secured target or group appears, listing user access rights to this secured target or group. Super auditors have access by default.
4. In the Modify Access page, select the users for which you want to grant or revoke access to this secured target or group.
5. Click **Grant Access** or **Revoke Access**.

   A check mark indicates access granted. An "x" indicates access revoked.
6. If necessary, repeat steps 4 and 5.
7. Click **Save**.

Changing a User Account Type in Oracle AVDF

You can change an auditor account type from auditor to super auditor, or vice versa. Note that if you change a user's account type from auditor to super auditor, that user will have access to all secured targets and secured target groups.

To change a user account type in Oracle AVDF:

1. Log in to the Audit Vault Server console as a super auditor.
2. Click the **Settings** tab.

   The Manage Auditors page appears by default, and displays existing users and the secured targets or groups to which they have access.

3. Click the name of the user account you want to change.
4. In the Modify Auditor page, in the **Type** section, click **Change**.
5. In the **Type** drop-down list, select the new auditor type.
6. If you changed the type from **Super Auditor** to **Auditor**, grant or revoke access to any secured targets or groups as necessary for this user:
   a. Select the secured targets or groups to which you want to grant or revoke access.
   b. Click **Grant Access** or **Revoke Access**.

      A check mark indicates access granted. An X indicates access revoked.
   c. Repeat steps a and b if necessary.
7. Click **Save**.

Deleting an Auditor Account in Oracle AVDF

As a super auditor, you can delete any auditor account except the last super auditor.

To delete an auditor user account:

1. Log in to the Audit Vault Server console as a super auditor.
2. Click the **Settings** tab.

   The Manage Auditors page appears by default, and displays existing users and the secured targets or groups to which they have access.
3. Select the users you want to delete, and then click **Delete**.

Changing Your Password

To change your Oracle AVDF password:

1. Log in to the Audit Vault Server console as an auditor.
2. Click the **Settings** tab, and then click **Change Password**.
3. Enter your **Current Password**, then enter your **New Password** twice, and then click **Save**.

   See also "About Oracle AVDF Auditor Accounts and Passwords" on page 3-1.

Creating Templates and Distribution Lists for Email Notifications

Topics

About Email Notifications and Templates

You can configure Oracle AVDF alerts to trigger an email when an alert is raised or a report is generated. For example, you can 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 AVDF

sends an email to two administrators warning them about misuse of the application account.

To accomplish this, you must create an email distribution list that defines who will receive the email, and then create an email template that contains a message. You select the template to be used for email notification when you define the alert rule.

Creating or Modifying an Email Distribution List

You can create an email distribution list for a specific notification purpose, that is, a list of email addresses that will receive a notification. You can specify a distribution list when notifying other users about alerts or reports.

To create or modify a distribution list:

1. Log in to the Audit Vault Server console as an auditor.
2. Select the **Settings** tab.
3. From the **Notifications** menu on the left, click **Distribution Lists**.

   The Distribution Lists page is displayed, showing existing lists, which you can modify or delete.
4. Click **Create** to add a new list, or click a list name to modify it, and then define the list as follows:
   - **Name** - Enter a name for the distribution list.
   - **Description** - (Optional) Enter a description of this list.
   - **To** - Enter the email addresses, separated by commas, that appear on the **To** line of notifications using this list.
   - **CC** - (Optional) Enter the email addresses, separated by commas, that appear on the **CC** line of notifications using this list.
5. Click **Save**.

   The new list appears in the Distribution Lists page. From there, you can modify or delete distribution lists as necessary.

Creating or Modifying an Email Template

An email template enables you to specify the content of an email notification that is triggered by an alert or a report being generated.

To create or modify an email template:

1. Log in to the Audit Vault Server console as an auditor, then click the **Settings** tab.
2. From the **Notifications** menu on the left, click **Email Templates**.

   The Email Templates page displays a list of existing email templates, which you can modify or delete. Some of these templates are predefined.
3. Click **Create** to create a new template, or click the name of an existing template to modify it.
4. Select the template **Type**:
   - **Alert:** Creates an email template used for alert notifications.
   - **Report Attachment:** Creates an email template used for report notifications, and attaches a PDF of the report to the email.

- **Report Notification:** Creates an email template used for report notifications, but does not attach the PDF file of the report.

5. Enter or select the desired values for **Name**, **Description**, and **Format** of this email template.
6. Use the available tags on the right as building blocks for the **Subject** and **Body** of the email.

   The available tags depend on the type of notification. Table 3–1 and Table 3–2 explain the tags in detail.

   For example, using these tags, you create this template:

   - For **Subject**, you enter `Report: #AlertName#, #DateCreated#`
   - For **Body**, you enter `The #ReportName# is ready for review at #URL#.`

   Then the following email notification may be generated:

   - **Subject:** `System Privileges Report, Sept 26, 2009, 3:15:06 PM`
   - **Body:** `The System Privileges Report is ready for review at http://mau.example.com/console/f?p=7700:4:3525486105242281::NO::P4_REPORT_ID:36`
7. Click **Save**.

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

Table 3–1 lists the available tags for alert notification templates.

Table 3–1 Tags Available for Alert Notification Email Templates

Alert Tag Name	Description
`#AlertBody#`	A special tag that is used as a shortcut to include all the available tags in the email
`#AlertID#`	The ID of the alert
`#AlertName#`	Name of the alert
`#AlertTime#`	Time the event causing the alert was created
`#AlertSeverity#`	Severity of the alert (**Critical** or **Warning**)
`#AlertStatus#`	Status of the Alert (for example, **New**, **Open**, or **Closed**)
`#Description#`	Description of the alert
`#EventTime#`	Timestamp of the event that raised the alert
`#URL#`	URL of the alert

Table 3–2 lists the available tags for report notification templates.

Table 3–2 Tags Available for Report Notification Email Templates

Report Tag Name	Description
`#ReportName#`	Name of the report
`#DateCreated#`	Date and time the report was generated
`#ReportCategory#`	Report Category name, such as "Access Reports"
`#URL#`	URL to the report that was generated

Viewing Enforcement Point and Audit Trail Status

Topics

Viewing Enforcement Point Status

To view enforcement points configured for all your secured target databases:

1. Log into the Audit Vault Server console as an auditor, and click the **Settings** tab or the **Secured Targets** tab.
2. From the **Quick Links** menu, click **Enforcement Points**.

   You can adjust the appearance of the list from the **Actions** menu. See "Working with Lists of Objects in the UI" on page 1-12.

Viewing Audit Trail Status

To view a list of audit trails collected for all your secured targets:

1. Log into the Audit Vault Server console as an auditor, and click the **Settings** tab or the **Secured Targets** tab.
2. From the **Quick Links** menu, click **Audit Trails**.

   Audit trails for all your secured target are listed in a table showing the trail, its status, the secured target name and type, and the host from which the trail was collected, the trail location and type.

   You can adjust the appearance of the list from the **Actions** menu. See "Working with Lists of Objects in the UI" on page 1-12.
3. Optionally, click a column title to sort by that column.

Monitoring Jobs

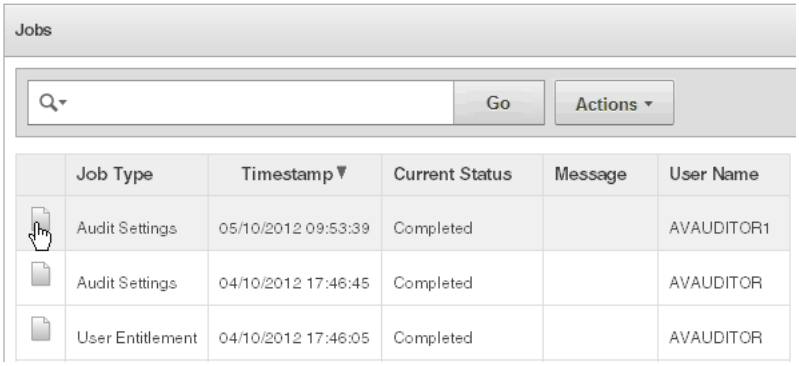
You can see the status of various jobs that run on the Audit Vault Server, such as report generation, and user entitlement or audit policy retrieval from secured targets.

To see the status of jobs in the Audit Vault Server:

1. Log in to the Audit Vault Server as an Auditor.
2. Click the **Settings** tab.
3. In the **System** menu, click **Jobs**.

   A list of jobs is displayed, showing the job type, ID, timestamp, status, and associated user name.
4. To see details for an individual job, click the icon to the left of that job. See Figure 3–1 below.

Figure 3–1 Jobs Page



4

Creating Database Firewall Policies

Topics

Overview of Database Firewall Policies

Topics

About Firewall Policies

Successful deployment of a Database Firewall depends on an effective policy. Oracle AVDF includes preconfigured firewall policies as described in the Firewall Policy page in the **Policy** tab of the Audit Vault Server console. For example, these include policies that log all SQL statements, or log only unique SQL statements. In addition, the Database Firewall policy editor enables you to design your own policies quickly and efficiently.

Policy rules can depend on any combination of the SQL statement type, name of the database user, IP address of the database client, operating system user name, client program name, or any exceptions you specify.

Developing a policy is an iterative process that keeps refining and improving the policy with new data.

The Steps of Developing a Firewall Policy

Developing a policy consists of these main steps:

1. Create a firewall policy in the Audit Vault Server. See "Creating a New Firewall Policy" on page 4-2.
2. Design your policy by setting policy actions and rules. See "Defining a Firewall Policy" on page 4-3.

3. Publish the policy to make it available for applying to secured targets. See "Publishing a Firewall Policy" on page 4-16.
4. Assign the policy to selected secured targets. "Deploying Firewall Policies to Secured Targets" on page 4-16.

Creating a Firewall Policy

Topics

Creating a New Firewall Policy

You can create a new firewall policy or copy an existing policy and edit it. See also "Copying a Firewall Policy" on page 4-2.

To create a new firewall policy:

1. Log in to the Audit Vault Server console as an auditor, and click the **Policy** tab.
2. Under the **Policy** menu, click **Firewall Policy**.
3. Click **Create Policy**.

   The Create Policy dialog appears.
4. Select the **Database Type** from the drop-down list.
5. Enter a **Policy Name**.
6. Optionally, enter a **Description**.
7. Click **Create**.

   The new policy is created, and the policy's Overview page appears. Next, see:

   - "Understanding a Firewall Policy's Overview Page" on page 4-3
   - "Defining a Firewall Policy" on page 4-3

Copying a Firewall Policy

You can copy an existing firewall policy and edit it to create a new policy. See also "Editing a Firewall Policy" on page 4-3.

To copy a firewall policy:

1. Log in to the Audit Vault Server console as an auditor, and click the **Policy** tab.
2. Under the **Policy** menu, click **Firewall Policy**.
3. Click the name of the policy you want to copy.

   The Policy Overview page appears.
4. Click **Copy**.
5. Enter a **Policy Name**, and then click **Copy**.

Editing a Firewall Policy

You can edit only firewall policies that you have created or copied.

To edit a firewall policy:

1. Log in to the Audit Vault Server console as an auditor, and click the **Policy** tab.
2. Under the **Policy** menu, click **Firewall Policy**.
3. Click the name of the policy you want to edit.

   The Policy Overview page appears.
4. Make your edits, referring to these topics for additional information:
   - "Understanding a Firewall Policy's Overview Page" on page 4-3
   - "Defining a Firewall Policy" on page 4-3
5. Click **Save**.

Understanding a Firewall Policy's Overview Page

When you create a new policy, or click an existing policy name in the Firewall Policies page, that policy's Overview page appears. This page shows the policy rules that are being applied to the statement types (clusters) being monitored by the Database Firewall, as well as exceptions and other rules that may apply.

The policy's Overview page is divided into these sub-sections:

- **Exception Rules** - Lists exceptions you have created. The rules that you have assigned to SQL statement clusters will not apply to these exceptions. You can move the rules up or down in the list. The rules are evaluated in the order listed. See "Creating Exceptions" on page 4-6.
- **Analyzed SQL** - Displays the number of SQL statement clusters for which you have defined policy rules, and their policy actions (such as Warn or Block). See "Defining Policy Rules for Analyzed SQL" on page 4-7.
- **Novelty Policies (Any)** - Lists special policies you have created for specific statement classes and/or specific tables in your secured target databases. If you have identified specific tables in a policy in this section, the policy rule applies if it matches **Any** of the tables. See "Creating Novelty Policies" on page 4-8.
- **Novelty Policies (All)** - Lists special policies you have created for specific statement classes and/or specific tables in your secured target databases. If you have identified specific tables in a policy in this section, the policy rule applies if it matches **All** of the tables. See "Creating Novelty Policies" on page 4-8.
- **Default Rule** - Shows the default rule for any statements that are not matched by the rules set for Analyzed SQL clusters, Exceptions, or Novelty Policies. See "Defining the Default Rule" on page 4-10.
- **Policy Controls** - Lets you configure firewall policy settings, create policy profiles, as well as sets of filters to use in defining profiles and Exception rules. See "Defining Session Filters to Use in Profiles and Exceptions" on page 4-5.

Defining a Firewall Policy

Topics

About Defining the Policy

To successfully deploy a Database Firewall you must develop an effective policy. Using the firewall policy editor, you can design and refine a policy based on analyzed SQL from traffic to your secured targets. Oracle AVDF analyzes SQL by looking at SQL traffic to all the secured target to which you have access. It then groups the SQL into clusters of similar statements, and displays these clusters in a firewall policy in the Audit Vault Server console.

You can then define the rules of your firewall policy based on these clusters. Defining rules for a firewall policy includes:

- Specifying these settings for each cluster in the analyzed SQL:
  - **Action:** Whether or not the Database Firewall permits, blocks, or produces a warning when it encounters a statement that matches the cluster.
  - **Logging level:** Whether the Database Firewall never logs, logs all statements, or logs statements that have a unique combination of cluster, source IP address, database username, operating system username, and client program name. You can use logging as an independent record of database activity, which may, for example, be used for future audit or forensic purposes.

    Consider the amount of logging carefully, because increasing the data logged directly impacts required disk space. The frequency for the sample logging is every tenth statement for the cluster.

    Oracle recommends that you use the "unique" logging level in policies for the initial policy because it guarantees one of each type. It efficiently samples traffic without logging all statements.
  - **Threat Severity:** The anticipated threat from statements in a cluster. There are five threat severity settings, ranging from Insignificant to Catastrophic (or Unassigned). When the Database Firewall logs a statement, the threat severity of the statement is also logged. You can use third-party reporting tools and syslogs to display SQL statements based on the logged threat severity.
- Creating Exceptions to the default policy settings for your analyzed SQL
- Adding Novelty Policies (or rules) that are triggered when specific statement types are encountered and/or selected tables are called
- Defining a Default Rule to handle any SQL that does not match any of your other policy rules.
- Creating Profiles to apply a different set of policy rules from your normal policy, based on specific criteria (such as client IP address)

Note: In blocking mode, by default the Database Firewall blocks all IPv6 traffic regardless of the policies in place.

Defining Session Filters to Use in Profiles and Exceptions

Policy controls let you create sets of filters, based on session information, to use in defining policy Profiles and Exception rules. For example, when defining an Exception rule you may want to exclude a set of database users from that rule, or apply the rule only if the SQL originates from specific IP addresses.

There are four types of filters for session information:

- **IP Address Sets:** A specified list of IP addresses of database clients (IPv4 format)
- **Database User Sets:** A specified list of database user login names
- **Database Client Sets:** A specified list of client programs, for example SQL*Plus.
- **OS User Sets:** A specified list of operating system user names

Before defining policy Profiles and Exceptions, you must first define these sets of session filters, then you can include or exclude them in Profiles or Exception rules. See:

- "Creating Exceptions" on page 4-6
- "Using Profiles to Customize a Firewall Policy" on page 4-14

To define session filters:

1. Log in to the Audit Vault Server console as an auditor, and select the **Policy** tab.
2. In the Firewall Policies page, click the name of the policy you want.
3. In the policy's Overview page, scroll down to the Policy Controls section, and click one of the following:
   - **IP Address Sets**
   - **Database User Sets**
   - **Database Client Sets**
   - **OS User Sets**

   The page for the selected policy control appears. For example, *Policy_Name* - IP Address Sets. This page lists the sets already defined for this policy control.
4. Click **Create New Set**.
5. In the dialog that appears enter a **New Set Name**, and the first member of the set:
   - For IP Address and Database Client sets, enter IP addresses.
   - For Database Client sets, enter the client program name.
   - For Database User and OS User sets, enter user names.
6. Click **Create Set**.

   The new set appears in the this policy control's page.
7. Add more members to the set by clicking the appropriate **Add** button for this set, for example, **Add DB Client**.

Creating Exceptions

Topics

About Exceptions

An exception determines the action, logging level, and threat severity to use when certain session data is encountered. For example, an exception could specify rules for statements that originate (or do not originate) from selected client IP addresses or database user names.

Exceptions override all other policy rules. For example, you may want to override the normal policy rules if SQL statements originate from an administrator, or if they originate from anywhere other than a specific IP address.

You can define many exceptions and control the order in which they are evaluated. Each Exception has its own Action, Logging, and Threat Severity settings.

In order to create an Exception, you must first define the sets of session factors to be used in defining it. See "Defining Session Filters to Use in Profiles and Exceptions" on page 4-5.

Creating Exceptions

To create an Exception:

1. In the Audit Vault Server console, select the **Policy** tab.
2. From the **Policy** menu, click **Firewall Policy**.
3. In the Firewall Policies page, click the name of the policy you want.
4. In the Exception Rules section, select **Add Exception**.
5. At the top of the Exception Rule page, select the filtering criteria for this exception:
   - **IP Address Set:** Select to **Include** or **Exclude**, then select an IP address set.
   - **DB User Set:** Select to **Include** or **Exclude**, then select an database user set.
   - **OS User Set:** Select to **Include** or **Exclude**, then select an OS user set.
   - **DB Client Set:** Select to **Include** or **Exclude**, then select a database client set.

   For example, if you select to **Include** an IP Address Set, and **Exclude** a DB User Set, then this exception rule will only apply to SQL from the selected IP Address Set, but will not apply to SQL from database users in the selected DB User Set.
6. In the bottom section of the Exception Rule page, assign the **Action**, **Logging Level**, and **Threat Severity** to apply to SQL matching this rule's filtering criteria.
7. (Optional) Select **Escalate action after a certain number of instances?** if you want to apply a different action after SQL matches this rule a number of times. Then enter the following:
   a. **Threshold:** Enter the number of times SQL must match this rule before the escalation action is taken.
   b. **Threshold Action:** Select Warn or Block as the action taken after the Threshold is met.

c. **Substitute Statement:** (Optional) If you selected **Block** for the **Threshold Action**, enter a statement to substitute for the SQL matching this rule. See "Blocking SQL and Creating Substitute Statements" on page 4-11 for advice.

8. (Optional) Enter a **Note**.
9. Click **Create**.

The Order of Applying Exceptions

Exception rules are applied in the order they are listed in the Policy Overview page. For example, if a statement matches an Exception definition in both the first and second exception rule, the Action, Logging, and Threat Severity of the first Exception is applied to that statement.

For this reason, it is more secure to have the more stringent action level in the first Exception, so an Exception with the action **Block** would supersede the Exception with the action **Warn**. In this case, if a statement matches both groups, it will be blocked.

> **Tip:** See also "Default Rule Settings in Relation to Other Policies" on page 4-11.

Defining Policy Rules for Analyzed SQL

Topics

About Analyzed SQL

In any firewall policy, you can see SQL from traffic to any secured targets to which you have access as an auditor. The Database Firewall analyzes SQL statements from traffic to any selected secured target and groups the statements into similar clusters. You can see a sample statement from each unique cluster in the Analyzed SQL section in the Policy Overview page of a firewall policy.

You can then select any sample statement and set policy rules for that type of statement. The rules include the action the Database Firewall should take (such as Warn or Block), the logging level, and the threat severity to indicate.

Defining Policy Rules for Analyzed SQL

To define firewall policy rules for Analyzed SQL:

1. In the Audit Vault Server console, click the **Policy** tab.
2. From the **Policy** menu, click **Firewall Policy**, and then the name of a policy.
3. In the Analyzed SQL section, click **Modify SQL**.

   The Modify SQL page appears, with no data displayed.
4. Click **Change**, select the options below, and then click **Apply**.
   - **Profile:** (Optional) Select a profile.
   - **Secured Target:** Select a secured target to see analyzed SQL for that target.
   - **Event Time:** Select time options in the available fields to filter the SQL.

A list of SQL clusters and their details and policy status is displayed. The SQL Statement column shows a sample statement from each cluster.

You can filter the list using the **Actions** menu. See "Working with Lists of Objects in the UI" on page 1-12.

5. (Optional) Select one of the following in the **Reports** drop-down list:
   - **Primary Report:** Displays all SQL clusters from traffic to your secured targets. If a cluster has a defined rule, a **Yes** appears in the In Policy column.
   - **SQL Statements in Policy:** Displays only the SQL clusters for which you have defined rules in this policy.
6. Select one or more clusters, and then click **Set Policy**.
7. In the Set Policy Controls dialog, select the **Action**, **Logging Level**, and **Threat Severity** to apply to SQL statements of this cluster type.
8. (Optional) Select **Escalate action after a certain number of instances?** if you want to apply a different action after a statement matches this cluster a number of times. Then enter the following:
   a. **Threshold:** Enter the number of times a SQL statement must match this cluster before the escalation action is taken.
   b. **Threshold Action:** Select Warn or Block as the action taken after the threshold is met.
   c. **Substitute Statement:** (Optional) If you selected **Block** for the **Threshold Action**, enter a statement to substitute for the SQL matching this cluster. See "Blocking SQL and Creating Substitute Statements" on page 4-11 for advice.
9. (Optional) Enter a **Note**.
10. Click **Save**.

    The In Policy column now has a **Yes** for the statement(s) for which you defined this rule. In the Policy Overview page, the Analyzed SQL section keeps a count of the total number of clusters that have policy rules defined, and the associated actions.

Analyzing SQL Encrypted with Oracle Network Encryption

Oracle Database provides network encryption. When enabled, this option automatically encrypts network traffic. In order for the firewall policy to analyze SQL encrypted using Oracle network encryption, the Oracle AVDF administrator must configure the Database Firewall to decrypt this traffic. See the *Oracle Audit Vault and Database Firewall Administrator's Guide* for information on how to do this configuration.

Creating Novelty Policies

Topics

About Novelty Policies

Novelty policies specify the action, logging level, and threat severity to use for specific types of statements and/or statements that operate on selected tables. Novelty policies can be used to loosen or tighten your normal policy rules if certain statements are encountered.

For example, if the normal policy action for a certain statement type is Warn, you may want to set up a novelty policy that applies a Pass action if this statement type operates on tables containing public information. Alternatively, you may want to set up a novelty policy that blocks all statements that operate on tables containing sensitive information.

Tip: See also, the following topics:

- "Novelty Policy Examples" on page 4-10
- "Default Rule Settings in Relation to Other Policies" on page 4-11

Creating Novelty Policies

To Create a Novelty Policy:

1. In the Audit Vault Server console, select the **Policy** tab.
2. From the **Policy** menu, click **Firewall Policy**.
3. In the Firewall Policies page, click the name of the policy you want.

   The Policy Overview page appears.
4. Click **Add Novelty Rule** in either of these sections:
   - **Novelty Policies (Any)** - If you add a novelty rule in this section, and you select specific tables in the rule, the novelty rule applies if a statement contains **Any** of the selected tables.
   - **Novelty Policies (All)** - If you add a novelty rule in this section, and you select specific tables in the rule, the novelty rule applies if **All** tables in the statement are selected in the rule. (Though you may select more tables than appear in the statement.)

   The **Novelty Policies (Any)** rules are evaluated before the **Novelty Policies (All)** rules. See "The Order of Applying Novelty Policies" on page 4-10 for more information.
5. In the Novelty Policy Details dialog, define the following:
   a. **Novelty Rule:** Enter a name for this rule.
   b. **Statement Classes:** (Optional) Select one or more types of statements that SQL statements must match in order to apply this rule.
   c. **Policy Controls:** Select the **Action**, **Logging Level**, and **Threat Severity** for this rule from the appropriate drop-down list.
   d. **Substitution:** (Optional) This field appears if you select Block as the **Action**. Enter a statement to substitute for the SQL statement that was blocked. See "Blocking SQL and Creating Substitute Statements" on page 4-11.
6. **Affected Tables:** (Optional) Select the table(s) to use for matching statements to this policy. The tables are matched according the Novelty Policy section chosen in Step 4.
7. Click **Create**.

The new Novelty Policy is listed in the appropriate **Novelty Policies** (Any or All) section.

The Order of Applying Novelty Policies

The Database Firewall first compares statements against the **Match Any Table** group of Novelty Policy rules. In a Match Any Table rule, at least one of the tables in a statement must match your selected table(s) for a statement to match the rule. If a statement matches more than one of the Match Any Table rules, the more severe policy is used. For example, a policy that blocks takes priority over a policy that warns.

If statements do not match a rule under the Match Any Table group, the Database Firewall then compares statements to the rules in the **Match All Tables** group. In a Match All Tables rule, all of the tables in the statement must be among your selected tables. Similarly, if a statement matches more than one rule in this group, the more severe action is applied.

If you create a Novelty Policy that only matches statement classes, but not tables, then the Novelty Policy will be evaluated with either the Match Any Table or Match All Tables group, depending on which one you select when defining the policy.

Novelty Policy Examples

There are two groups of Novelty Policies in a firewall policy. They appear in the Novelty Policies (Any) and Novelty Policies (All) sections of the Policy Overview page, and are evaluated in that order. See "The Order of Applying Novelty Policies" on page 4-10.

The following are examples of how Novelty Policy rules work:

- You create a Novelty Policy in the **Novelty Policies (Any)** section. The Novelty Policy rules in this section are evaluated first.

  For Statement Classes, you select Composite with Transaction. You also select the tables `AVG_COST`, `BOOKS`, and `BUSINESS_CONTACTS`.

  A statement that matches this rule must be in the Composite with Transaction class AND it must contain **any** of the tables you selected. This rule will be evaluated with the group of novelty policy rules in this section. This group of rules is evaluated first.

- You create a Novelty Policy in the **Novelty Policies (All)** section. The Novelty Policy rules in this section are evaluated second.

  For Statement Classes, you select Procedural and Composite. You also select the tables `AVG_COST`, `BOOKS`, and `BUSINESS_CONTACTS`.

  A matching statement must be in either the Procedural or Composite class AND **all** the tables in the statement must match at least one of the tables `AVG_COST`, `BOOKS`, or `BUSINESS_CONTACTS`. So the statement may have one, two, or all three of these tables. However, if a different table appears in the statement, it will not match this rule.

Defining the Default Rule

Topics

About the Default Rule

The Default Rule lets you specify the Action, Logging Level, and Threat Severity for any statement that does not fall into any of your other policy rules. When the Database Firewall encounters such a statement, it will apply the Default Rule.

Optionally, you can apply a different action in the Default Rule after a number of similar statements are seen per minute, and/or provide a substitute statement.

Default Rule Settings in Relation to Other Policies

If you set the action for the Default Rule to Block, setting the action of a Novelty Policy, Exception, or the Invalid Statement policy to Pass or Warn will weaken the blocking action of the Default Rule, and therefore the security of your firewall policy overall.

Defining the Default Rule

To define the Default Rule:

1. In the Audit Vault Server console, select the **Policy** tab.
2. From the **Policy** menu, click **Firewall Policy**.
3. In the Firewall Policies page, click the name of the policy you want.

   The Policy Overview page appears.
4. Scroll down to the Default Rule section, and click the **Default Rule** link.
5. In the Edit Default Rule page, assign the **Action**, **Logging Level**, and **Threat Severity**.
6. (Optional) Select **Escalate action after a certain number of instances?** if you want to apply a different action after statements fall within the default rule a number of times. Then enter the following:
   a. **Threshold:** Enter the number of times SQL must fall within the default rule before the escalation action is taken.
   b. **Threshold Action:** Select Warn or Block as the action taken after the Threshold is met.
   c. **Substitution:** (Optional) If you selected **Block** for the **Threshold Action**, enter a statement to substitute for the SQL matching this rule. See "Blocking SQL and Creating Substitute Statements" on page 4-11 for advice.
7. Click **Apply Changes**.

Blocking SQL and Creating Substitute Statements

When the Database Firewall is in DPE (or blocking) mode, you can configure a firewall policy to block certain SQL statements.

When you block SQL statements, you may also substitute a different SQL statement for any statement that is blocked. A substitute statement may be necessary to ensure that the database client is presented with an appropriate error message or response when a statement is blocked.

Note the following when blocking or writing substitute statements:

- **Blocking or warning when statements occur a specified number of times:** You can choose to block the SQL statement or produce a warning if a statement that matches the selected cluster occurs a specified number of times (or threshold value). You should always enable logging for blocked statements.

- **Creating substitute SQL statements:** You must be sure that the results of the substitute statement can be handled by your client applications.

  The following is an example of a good substitute statement you can use for an Oracle Database secured target. This statement is harmless and does not return any values or affect performance.

  ```
  SELECT 100 FROM DUAL
  ```

Configuring Other Policy Settings

Topics

Creating Login and Logout Policies for Database Users

You can specify the login and logout policies for database users. These policies send alerts when the rules you set for logins and logouts are violated. This is useful in the case of automated attacks on the database. You can configure the system to produce an alert when a database user logs in or out, and block database users who make a specified number of unsuccessful logins attempts.

> **Note:** In order to use a Login/Logout policy for a secured target database, you must activate database response monitoring in the settings of the enforcement point monitoring that database. See *Oracle Audit Vault and Database Firewall Administrator's Guide* for instructions.

To configure the login and logout policies:

1. In the Audit Vault Server console, select the **Policy** tab.
2. From the **Policy** menu, click **Firewall Policy**.
3. In the Firewall Policies page, click the name of the policy you want.

   The Policy Overview page appears.
4. Scroll down to the Policy Controls section, and click **Settings**.
5. In the Login/Logout Policy section, configure the following:
   - **Login Policy:** Specify the **Action** level and **Threat Severity** to use for successful or unsuccessful database user logins, and whether to **Enable Logging** for logins.
   - **Failed Login Policy:** Optionally, select **Enable failed login policy escalation**. This lets you produce an alert, or block a client, after a specified number of consecutive unsuccessful logins. If triggered, login blocking continues for the specified **Reset period**. After this period, the database client can attempt to log in again.
   - **Logout Policy:** Specify the **Action** level and **Threat Severity** to use for successful or unsuccessful database user logouts, and whether to **Enable Logging** for logouts.

6. Click **Save** in the Login/Logout Policy section.

Masking Sensitive Data

The Database Firewall obfuscates all passwords. In addition, you can set rules for masking other sensitive data. Sensitive data masking prevents sensitive data, such as credit card numbers, from appearing in log files. If a logged statement matches your data masking policy, the policy automatically replaces all user data in that statement (such as, string constants, integer constants, hexadecimal constants, and float constants) with alternative characters. The characters used depend on the data type.

Note: Once sensitive data is masked, it cannot be unmasked.

To set rules for sensitive data masking:

1. In the Audit Vault Server console, select the **Policy** tab.
2. From the **Policy** menu, click **Firewall Policy**.
3. In the Firewall Policies page, click the name of the policy you want.

   The Policy Overview page appears.
4. Scroll down to the Policy Controls section, and click **Settings**.
5. In the Sensitive Data Masking section, configure the following:
   a. Select or deselect **Mask sensitive data**.
   b. Select either **For all statements**, or **Only for statements matching the following criteria**.
   c. If you selected to mask based on criteria, enter the criteria:

      Having columns: Enter the database columns.

      Having procedures: Select **Any** or enter the procedures.
   d. Select whether to **Include invalid statements**.
   e. Click **Save** in the Sensitive Data Masking section.

Setting a Policy for Invalid SQL

You can set policy rules for SQL statements that are not recognized, such as statements that do not conform to the SQL syntax.

To set policy rules for invalid SQL:

1. In the Audit Vault Server console, select the **Policy** tab.
2. From the **Policy** menu, click **Firewall Policy**.
3. In the Firewall Policies page, click the name of the policy you want.

   The Policy Overview page appears.
4. Scroll down to the Policy Controls section, and click **Settings**.
5. In the Invalid Statement Policy section, assign the **Action**, **Logging Level**, and **Threat Severity**.
6. (Optional) Select **Escalate action after a certain number of instances?** if you want to apply a different action after invalid SQL statements are seen a number of times. Then enter the following:

a. **Threshold:** Enter the number of times invalid SQL must be seen before the escalation action is taken.

b. **Threshold Action:** Select Warn or Block as the action taken after the Threshold is met.

c. **Substitution:** (Optional) If you selected **Block** for the **Threshold Action**, enter a statement to substitute for the invalid SQL. See "Blocking SQL and Creating Substitute Statements" on page 4-11 for advice.

Configuring Global Firewall Policy Settings

To configure global settings for a firewall policy:

1. In the Audit Vault Server console, select the **Policy** tab.
2. From the **Policy** menu, click **Firewall Policy**.
3. In the Firewall Policies page, click the name of the policy you want.

   The Policy Overview page appears.
4. Scroll down to the Policy Controls section, and click **Settings**.
5. In the Global Settings section, configure the following:

   a. Under Logging, select whether to **Strip binary objects and comments from log files**.

   b. Under Policy, in the **Threshold action reset time (minutes)** field, enter a number of minutes. If you have set a **Threshold** in any of your policy rules, and the **Threshold Action** in your rule is taken, the action will not be repeated for the time you specify here. This prevents too many block/warn actions for the same rule.

   c. Under Policy, in the **Without substitution set block action to** field, select the action to take (**No response** or **Drop connection**) if one of your policy rules is set to Block and you have not specified a substitute statement in the rule.

   d. Under Syntax, select whether to **Treat double quoted strings as identifiers**. This determines whether double-quoted strings in SQL statements are treated as identifiers or string constants. If you deselect this check box, sensitive data masking (if used) will mask text in double quotes.

   e. Under Case, select whether this firewall policy does **Case sensitive matching for** client program names, database user names, and/or OS user names.
6. Click **Save** in the Global Settings section.

Using Profiles to Customize a Firewall Policy

Topics

About Profiles

Within a firewall policy, a profile lets you define a different set of policy rules based on the session data associated with SQL statements.

To define the profile, you use the session filters you defined in the Policy Controls section of the firewall policy. see "Defining Session Filters to Use in Profiles and Exceptions" on page 4-5.

These session filters filter SQL statements based on:

- **IP addresses**
- **Database user login names**
- **Client program names** (for example, SQL*Plus)
- **Operating system user names**

A profile is different from an exception, though they are both defined using the above session factors. Whereas an exception lets you bypass all the rules for Analyzed SQL in your normal policy, a profile lets you define rules for any cluster in the Analyzed SQL based on the session factors.

For example, you can create a profile if you want to define a completely different set of rules for Analyzed SQL originating from a certain set of database users. When a user in this database user set accesses the database, this profile's policy rules are used instead of your normal policy rules.

A SQL statement can match more than one profile. In this case, the Database Firewall uses the most severe action, logging level, and threat severity of all matching profiles.

Creating a Profile

In order to create a profile, there must be sets of factors defined to use for filtering purposes. See "Defining Session Filters to Use in Profiles and Exceptions" on page 4-5.

To create a Profile:

1. Log in to the Audit Vault Server console as an auditor, and select the **Policy** tab.
2. In the Firewall Policies page, click the name of the policy you want.
3. In the Policy Controls section of the page, click **Profiles**.

   The Policy Profiles page appears, listing existing profiles. You can click a profile name to edit it.
4. Click **Create New Profile**.
5. In the Create Profile dialog, enter the following:
   - **Profile Name:** Enter a name for the profile.
   - **IP Address Set:** Select one of the available IP address sets, or leave it unselected.
   - **DB User Set:** From the list, select from the available database user sets, or leave it unselected.
   - **OS User Set:** From the list, select from the available operating system user sets, or leave it unselected.
   - **DB Client Set:** From the list, select from the available client program sets, or leave it unselected.

   Note: Client program names and OS user names are provided by the client and therefore, depending on the environment, may not be reliable.

6. Click **Create Profile**.

   The profile appears in the Analyzed SQL section of the Policy Overview page. You can now select this profile and set policy rules for the Analyzed SQL. These rules will supersede your normal rules when this profile is matched. See "Defining Policy Rules for Analyzed SQL" on page 4-7.

Publishing and Deploying Firewall Policies

Topics

About Publishing and Using Firewall Policies

You can edit a firewall policy as much as you need to before publishing it. Publishing a policy makes it available to assign to secured targets.

Once a firewall policy is assigned to a secured target, it cannot be edited. However, you can copy the policy and continue refining it under another name. Once you are happy with the new refined policy, you can publish it and assign it to secured targets.

Publishing a Firewall Policy

To publish a firewall policy:

1. In the Audit Vault Server console, click the **Policy** tab.
2. From the **Policy** menu, click **Firewall Policy**, and then click the name of the policy you want to publish.
3. Click **Publish**.

   A firewall policy publish job is started. You can check the status of the publish job by clicking **Jobs** in the **Settings** tab.

   Once the policy is published, it is available to select in secured target pages. See "Deploying Firewall Policies to Secured Targets" on page 4-16.

Deploying Firewall Policies to Secured Targets

To assign a firewall policy to a secured target:

1. In the Audit Vault Server console, click the **Secured Targets** tab.
2. In the Targets page, click the name of the secured target you want.
3. In the Secured Target Details page, expand the Firewall Policy section and click **Change**.
4. From the drop-down list, select the policy you want, and then click **Save**.

   The new policy name appears, and on the Firewall Policy page (in the **Policy** tab), a **Yes** appears in the **Deployed** column for this policy.

5

Creating Audit Policies for Oracle Databases

Topics

About Audit Policies

Using the Audit Vault Server console, you can retrieve audit policies from Oracle database secured targets. You can then modify the policies or create new ones, and then provision them to the Oracle databases. You can retrieve and modify the following types of Oracle Database audit policies.

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

> **Note:** Although Oracle AVDF can collect data from the v$unified_audit_trail in Oracle Database 12*c*, Oracle AVDF cannot retrieve or provision unified audit policies.

General Steps for Creating Audit Policies for Oracle Databases

In general, to create audit policies for Oracle databases, you perform the following steps as described in this chapter:

1. Retrieve the current audit policy settings from the secured target Oracle database, and specify which of the current settings are needed.
2. If necessary, define more audit policy settings to add to the needed settings.
3. Provision the audit policy to the secured target database. The policy settings you specified as needed, and the new ones you created, then become the policies in use in the database.

Retrieving and Modifying Audit Settings from an Oracle Database

Topics

Understanding the Columns on the Audit Settings Page

Each time you retrieve the audit settings from a secured target Oracle database, you see the state of the database audit settings at that point in time. The Audit Settings page in the Audit Vault Server (in the **Policy** tab) shows an overview of the audit settings in use at secured target Oracle Databases, and shows any differences between those and the settings you have set as needed in your Oracle AVDF audit policies for those databases. You can then specify which of the current settings are needed.

Table 5–1 describes the columns shown in the Audit Settings Page.

Table 5–1 Fields Under Apply Audit Settings in the Audit Settings Page

Column	Description
Target Name	Name of the secured target
In Use	Number of audit settings in use in the secured target
Needed	Number of audit settings you (the auditor) specified as needed
Problem	The difference between the audit settings in use at the database and the number specified as needed in your Oracle AVDF audit policy for this database. If this number is greater than zero, new audit settings may have been created at the database since you last provisioned the audit policy from Oracle AVDF. You may also have selected more audit settings as needed or not needed since you last provisioned the audit policy. To resolve the problem, you can specify whether new audit settings are needed and/or provision the policy again. This brings the number in the **Problem** column back to zero.
Last Retrieved	The time that the audit information for the selected database was last retrieved
As Provisioned	The time that the audit settings were last provisioned to the database from Oracle AVDF

Retrieving Audit Settings from an Oracle Database

To retrieve audit settings from an Oracle Database secured target:

1. Log in to the Audit Vault Server console as an auditor.
2. Click the **Policy** tab.

   By default, the Audit Settings page appears. A summary of audit settings at this point in time is displayed for that secured target. For each secured target, this page lists the status of the audit policies. See "Understanding the Columns on the Audit Settings Page" on page 5-2.
3. From the **Target Name** column, select the check boxes for the secured target databases you want.

   You can only see the Oracle database secured targets to which you have access.

Note: Audit trails and audit policy management are not supported for Oracle Database 9*i*.

4. Click the **Retrieve Audit Settings** button.

   To check the status of the retrieval, click the **Settings** tab, then under the **System** menu, click **Jobs**. When the audit settings retrieval is complete, the Audit Settings page is refreshed with new data.

Specifying Which Audit Settings Are Needed

After you retrieve the audit settings from the secured target Oracle database, you can view and modify them as needed. Remember that you are modifying audit settings in use at the time you retrieved them. If you think they may have changed, you should retrieve them again. See "Retrieving Audit Settings from an Oracle Database" on page 5-2.

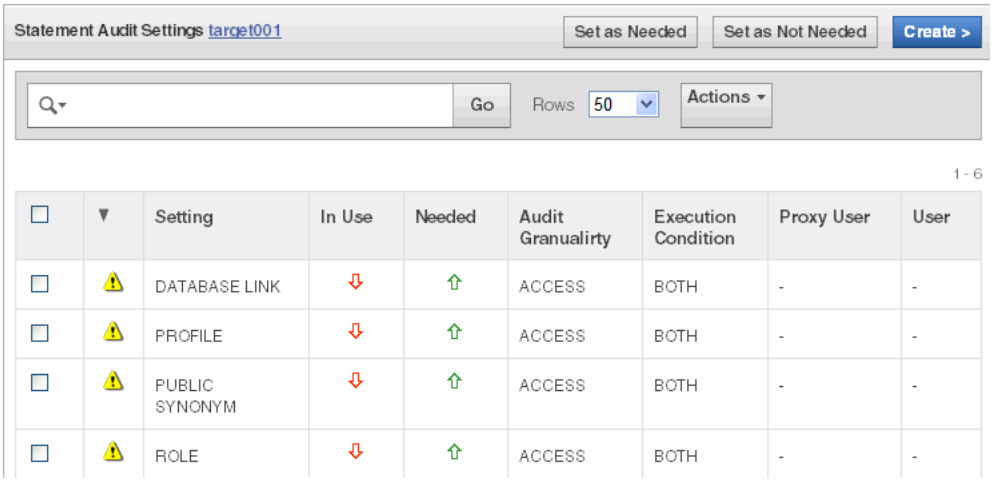
1. In the Audit Settings page, click the name of the secured target database you want.

   The Audit Settings Overview page for this secured target appears, showing the audit settings in use and marked as needed for these audit types:

   - Statement
   - Object
   - Privilege
   - FGA
   - Capture Rule

2. To update settings for any audit type, click its link, for example, **Statement**.

   The Audit Settings page for that audit type appears, listing the current audit settings. The second column displays a problem icon if there is a difference between the setting at the secured target database, and the setting in Oracle AVDF.



3. Select the checkboxes for each audit setting you determine is needed, then click **Set as Needed**.

4. To remove audit settings, select the checkboxes for the ones you want to remove, then click **Set as Not Needed**.

5. To create new audit settings for this audit type (for example, Statement), click **Create**. See "Creating Additional Audit Policy Settings for an Oracle Database" on page 5-4.

Creating Additional Audit Policy Settings for an Oracle Database

Topics

About Creating Audit Policy Settings

Once you have retrieved audit policy settings from the secured target Oracle database, and selected which of the settings in use are needed, you can also create new policy settings for the Oracle database.

Creating Audit Policies for SQL Statements

Topics

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.

Defining SQL Statement Audit Settings

To define SQL statement audit settings:

1. Log in to the Audit Vault Server console as an auditor.
2. If necessary, retrieve and update the current audit settings.

See "Retrieving and Modifying Audit Settings from an Oracle Database" on page 5-2 for more information.

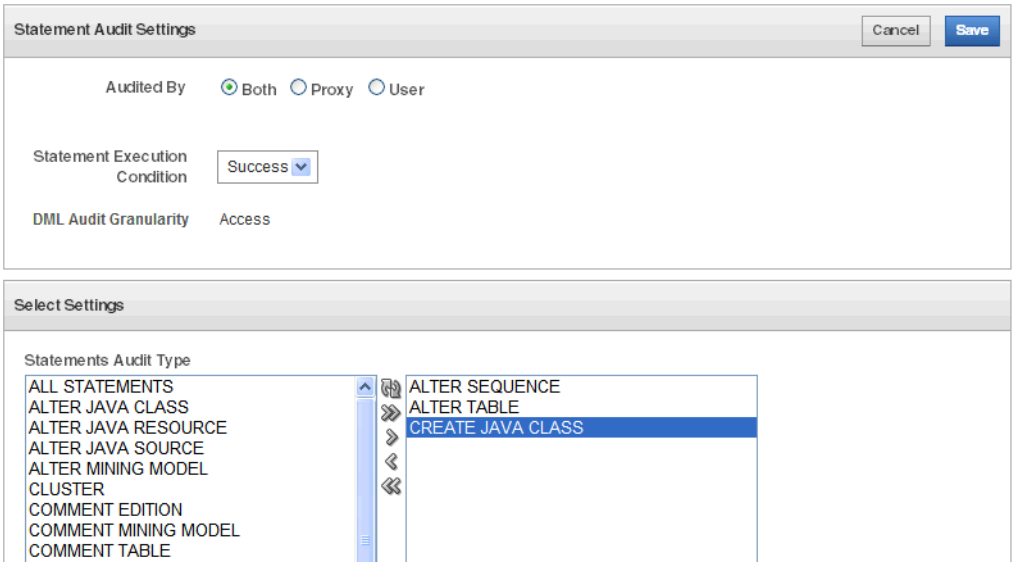
3. Click the **Policy** tab, and in the Audit Settings page, click an Oracle Database secured target.

   The target's Audit Settings Overview page is displayed.

4. Click **Statement**.

   The Statement Audit Settings page appears. See "Understanding the Statement Audit Settings Page" on page 5-6.

5. Click the **Create** button.



6. In the Create page, define the audit policy as follows:

   - **Audited By** - Choose the users to audit:
     - **Both:** Audits all users, including proxy users.
     - **Proxy:** 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 secured targets for selection, click the up-arrow icon on the right of the field.
     - **User:** Audits the user to which this setting applies. If you select this option, you must select a user from the **Users** drop-down list.
   - **Statement Execution Condition** - Choose one of the following:
     - **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 audit granularity for DML statements:
     - **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

     DDL statements are always audited by access.

- **Statements Audit Type** - Select the SQL statements to audit by double clicking a statement type to move it to the box on the right. You can use the double arrows to move all statements to the right or back to the left.

7. Click **Save**.

   The new audit settings are added to the Statement Audit Settings page.

Understanding the Statement Audit Settings Page

Table 5–2 lists the columns used in the Statement page.

Table 5–2 Columns in the Statement Audit Settings Page

Column	Description
(Leftmost column)	A checkbox for selecting the audit setting
Problem icon	An exclamation mark icon indicates one of the following conditions: ■ The setting is marked as needed in Oracle AVDF, but is not in use in the secured target database. ■ The setting is in use at the secured target database, but is not marked as needed in Oracle AVDF.
Setting	The statement that is audited
In Use	The arrow points upward if the setting is active in the secured target database, and downward if it has not been provisioned or is not active.
Needed	The arrow points upward if the audit setting is marked as needed in Oracle AVDF, and downward if the audit setting is marked as not needed. If an audit setting that is not in use is set to needed, the **In Use** arrow points up after provisioning. If an audit setting that is in use is set to not needed, the audit setting is no longer displayed after provisioning.
Audit granularity	The granularity of auditing: `BY ACCESS` or `BY SESSION`
Execution Condition	The execution condition audited: `SUCCESS`, `FAILURE`, or `BOTH`
Proxy User	The proxy user for the database, if any
User	The user to which this setting applies, if any

Creating Audit Policies for Schema Objects

Topics

- About Schema Object Auditing
- Defining Schema Object Audit Settings
- Understanding the Object Audit Settings Page

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 sets schema object audit options for all users of the database. You cannot set these options for a specific list of users.

Defining Schema Object Audit Settings

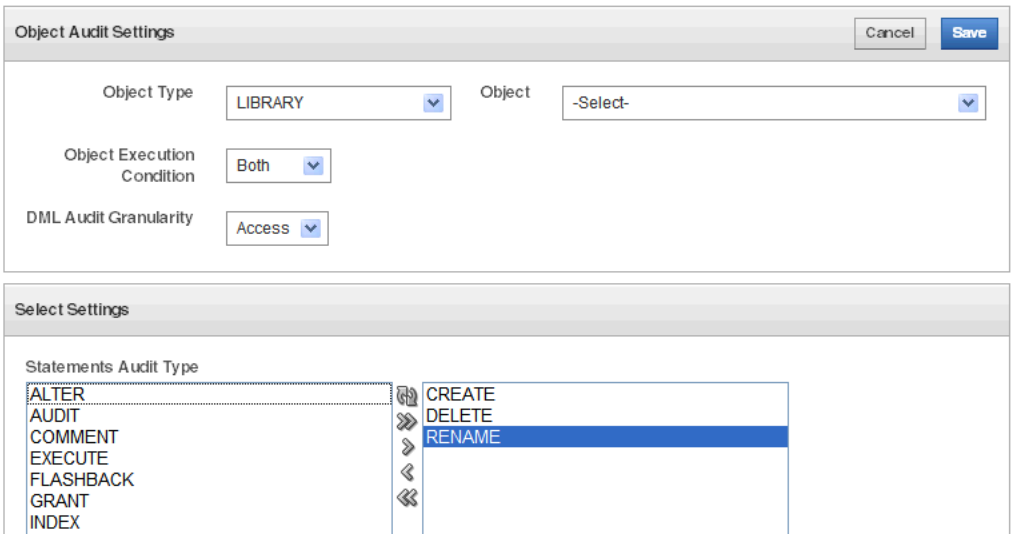
To define schema object audit settings:

1. Log in to the Audit Vault console as an auditor.
2. If necessary, retrieve and update the current audit settings.

   See "Retrieving and Modifying Audit Settings from an Oracle Database" on page 5-2 for more information.
3. Click the **Policy** tab, and in the Audit Settings page, click a secured target Oracle database.

   The target's Audit Settings Overview is displayed.
4. Click **Object** to display the Object Audit Settings page.

   See "Understanding the Object Audit Settings Page" on page 5-8 for descriptions of the columns used in this page.
5. Click the **Create** button.



6. In the Object Audit Settings page, define the settings as follows:
   - **Object Type** - Select the type of object to audit from the drop-down list, such as TABLE, LOB, RULE, or VIEW.
   - **Object** - Select a specific object of the object type you selected.
   - **Object Execution Condition** - Choose one of the following:
     - **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 audit granularity for DML statements:
  - **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

  DDL statements are always audited by access.
- **Statements Audit Type** - Select the SQL statements to audit by double clicking a statement type to move it to the box on the right. You can use the double arrows to move all statements to the right or back to the left.

7. Click **Save**.

   The new object audit settings are added to the Object Audit Settings page.

Understanding the Object Audit Settings Page

Table 5–3 lists the columns used in the Object page.

Table 5–3 Columns in the Object Audit Settings Page

Column	Description
(Leftmost column)	A checkbox for selecting the audit setting
Problem icon	An exclamation mark icon indicates one of the following conditions: ■ The setting is marked as needed in Oracle AVDF, but is not in use in the secured target database. ■ The setting is in use at the secured target database, but is not marked as needed in Oracle AVDF.
Setting	The statement that is audited
In Use	The arrow points upward if the setting is active in the secured target database, and downward if it has not been provisioned or is not active.
Needed	The arrow points upward if the audit setting is marked as needed in Oracle AVDF, and downward if the audit setting is marked as not needed. If an audit setting that is not in use is set to needed, the **In Use** arrow points up after provisioning. If an audit setting that is in use is set to not needed, the audit setting is no longer displayed after provisioning.
Object Type	The object (such as a database table) to which this setting applies
Object Owner Name	The database schema to which this setting applies
Object Name	The name of the object in the specified schema.
Audit granularity	The granularity of auditing: `BY ACCESS` or `BY SESSION`
Execution Condition	The execution condition audited: `SUCCESS`, `FAILURE`, or `BOTH`

Creating Audit Policies for Privileges

Topics

- About Privilege Auditing

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.

Defining Privilege Audit Settings

To define create privilege audit settings:

1. Log in to the Audit Vault Server console as an auditor.
2. If necessary, retrieve and update the current audit settings.

   See "Retrieving and Modifying Audit Settings from an Oracle Database" on page 5-2 for more information.
3. Click the **Policy** tab, and in the Audit Settings page, click a secured target Oracle database.

   The target's Audit Settings Overview is displayed.
4. Click **Privilege** to display the Privilege Audit Settings page.

   See "Understanding the Privilege Audit Settings Page" on page 5-10 for descriptions of the fields used in this page.
5. Click the **Create** button, and in the Create Privilege Audit page, define the privilege audit policy as follows:
   - **Audited By** - Choose the users to audit:

  - **Both:** Audits all users, including proxy users.
  - **Proxy:** 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 secured targets for selection, click up-arrow icon on the right of the field.
  - **User:** Audits the user to which this setting applies. When you select this option, the **Users** field appears, and you must specify a user from the drop-down list.
- **Statement Execution Condition** - Choose one of the following:
  - **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 audit granularity for DML statements:
  - **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

  DDL statements are always audited by access.
- **Statements Audit Type** - Select the privileges to audit by double clicking a statement type to move it to the box on the right.

  You can use the double arrows to move all statements to the right or back to the left.

6. Click **Save**.

   The new privilege audit settings are added to those listed in the Privilege Audit Settings page.

Understanding the Privilege Audit Settings Page

Table 5–4 lists the columns used in the Privilege Audit Settings page.

Table 5–4 Columns in the Privilege Audit Settings Page

Column	Description
(Leftmost column)	A checkbox for selecting the audit setting
Problem icon	An exclamation mark icon indicates one of the following conditions: ■ The setting is marked as needed in Oracle AVDF, but is not in use in the secured target database. ■ The setting is in use at the secured target database, but is not marked as needed in Oracle AVDF.
Setting	The statement that is audited
In Use	The arrow points upward if the setting is active in the secured target database, and downward if it has not been provisioned or is not active.

Table 5–4 (Cont.) Columns in the Privilege Audit Settings Page

Column	Description
Needed	The arrow points upward if the audit setting is marked as needed in Oracle AVDF, and downward if the audit setting is marked as not needed. If an audit setting that is not in use is set to needed, the **In Use** arrow points up after provisioning. If an audit setting that is in use is set to not needed, the audit setting is no longer displayed after provisioning.
Audit granularity	The granularity of auditing: `BY ACCESS` or `BY SESSION`
Execution Condition	The execution condition audited: `SUCCESS`, `FAILURE`, or `BOTH`
User	The user to which this setting applies, if any
Proxy User	The proxy user for the database, if any

Creating Audit Policies for Fine-Grained Auditing (FGA)

Topics

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.

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, 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.

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 email 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.

Defining Fine-Grained Audit Settings

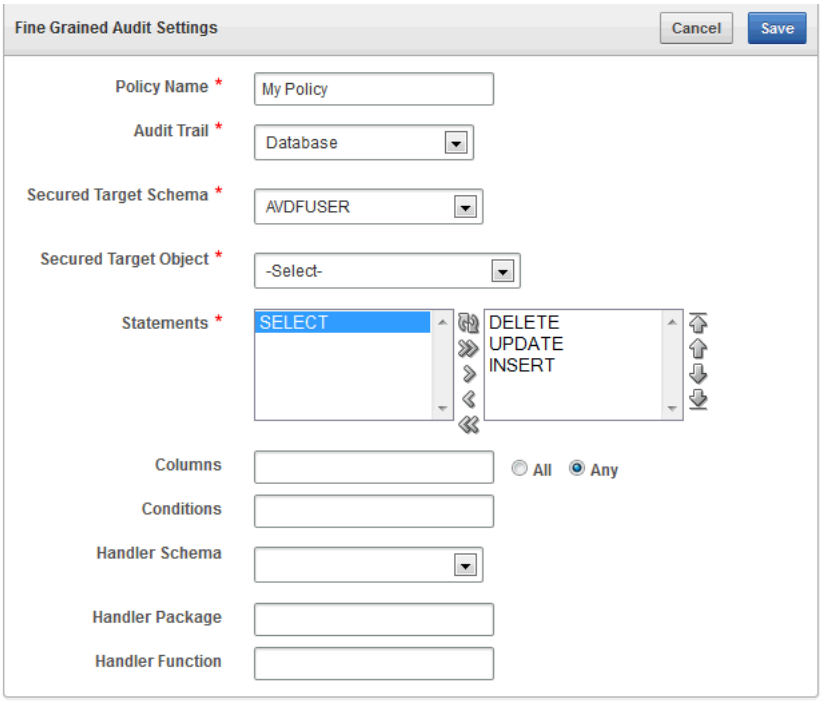
To define fine-grained audit settings:

1. Log in to the Audit Vault Server console as an auditor.
2. If necessary, retrieve and update the current audit settings.

   See "Retrieving and Modifying Audit Settings from an Oracle Database" on page 5-2 for more information.
3. Click the **Policy** tab, and in the Audit Settings page, click a secured target Oracle database.

   The database's Audit Settings Overview is displayed.
4. Click **FGA** to display the Fine Grained Audit Settings page.

   See "Understanding the Fine-Grained Audit Settings Page" on page 5-14 for descriptions of the fields used in this page.
5. Click the **Create** button.



6. Define the audit policy as follows:

   - **Policy Name** - Enter a name for this fine-grained audit policy.
   - **Audit Trail** - Select from one of the following audit trail types:
     - **Database:** Writes the policy records to the database audit trail `SYS.FGA_LOG$` system table.
     - **Database with SQL Text:** Performs the same function as the Database option, but also populates the SQL bind and SQL text CLOB-type columns of the `SYS.FGA_LOG$` table.
     - **XML:** Writes the policy records to an operating system XML file. To find the location of this file, a database administrator can run the following command in SQL*Plus:

       SQL> SHOW PARAMETER AUDIT_FILE_DEST
     - **XML with SQL Text:** Performs the same function as the XML option, but also includes all columns of the audit trail, including `SQLTEXT` and `SQLBIND` values.

     WARNING: Be aware that sensitive data, such as credit card numbers, appear in the audit trail if you collect SQL text.

   - **Secured Target Schema** - Select a schema to audit.
   - **Secured Target Object** - Select an object to audit.
   - **Statements** - Select one or more SQL statements to audit by double clicking each statement to move it to the box on the right. You can select: `DELETE`, `INSERT`, `MERGE`, `SELECT`, or `UPDATE`.
   - **Columns** - (Optional) Enter the names of the database columns (relevant columns) to audit. Separate each column name with a comma. If you enter

more than one column, select **All** or **Any** as the condition that triggers this policy.

See "Auditing Specific Columns and Rows" on page 5-11 for more information about relevant columns.

- **Conditions** - (Optional) Enter a Boolean condition to filter row data. For example, `department_id = 50`.

  If this field is blank or null, auditing occurs regardless of condition.

- **Handler Schema** - (Required if you specify an event handler function) Enter the name of the schema account in which the event handler was created. For example: `SEC_MGR`

  See "Using Event Handlers in Fine-Grained Auditing" on page 5-12.

- **Handler Package** - (Required if you specify an event handler function) Enter the name of the package in which the event handler was created. For example: `OE_FGA_POLICIES`

- **Handler Function** - (Optional) Enter the name of the event handler. For example: `CHECK_OE_VIOLATIONS`

7. Click **Save**.

   The fine-grained audit policy is created.

Understanding the Fine-Grained Audit Settings Page

Table 5–5 lists the columns used in the Fine-Grained Audit Settings page.

Table 5–5 Columns in the Fine-Grained Audit Settings Page

Field	Description
(Leftmost column)	A checkbox for selecting the audit setting
Problem icon	An exclamation mark icon indicates one of the following conditions: ▪ The setting is marked as needed in Oracle AVDF, but is not in use in the secured target database. ▪ The setting is in use at the secured target database, but is not marked as needed in Oracle AVDF.
Policy Name	The name of this fine-grained audit policy
In Use	The arrow points upward if the setting is active in the secured target and downward if it has not been provisioned or is not active.
Needed	The arrow points upward if the audit setting is marked as needed in Oracle AVDF, and downward if the audit setting is marked as not needed. If an audit setting that is not in use is set to needed, the **In Use** arrow points up after provisioning. If an audit settings that is in use is set to not needed, the audit setting is no longer displayed after provisioning.
Object Owner	The schema to which this audit setting applies
Object	The object, in the specified schema, to which this audit setting applies

Table 5–5 (Cont.) Columns in the Fine-Grained Audit Settings Page

Field	Description
Statement Types	The SQL statement to which this audit setting applies. Values are: ■ 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.

Creating Capture Rules for Redo Log File Auditing

Topics

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 secured target, because you cannot create them there. You only can create the capture rule in the Audit Vault Server console.

> **Note:** In the secured target 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.

Defining a Capture Rule for Redo Log File Auditing

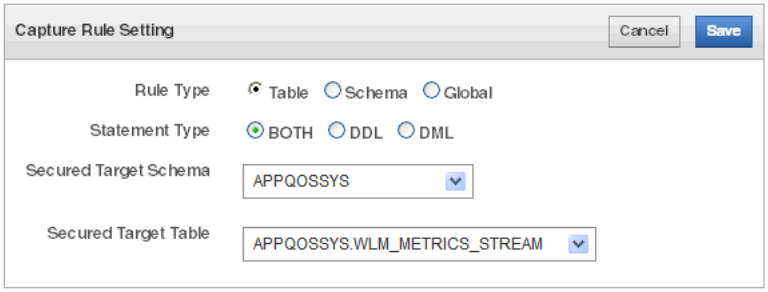
To define a capture rule:

1. Log in to the console as an auditor.
2. If necessary, retrieve and update the current statement audit policies.

   See "Retrieving and Modifying Audit Settings from an Oracle Database" on page 5-2 for more information.
3. Click the **Policy** tab, and in the Audit Settings page, click a secured target Oracle database.

   The target's Audit Settings Overview is displayed.
4. Click **Capture Rule** to display the Capture Rule Settings page.

   See "Understanding the Capture Rule Settings Page" on page 5-16 for descriptions of the fields used in this page.
5. Click the **Create** button.



6. Define the capture rule as follows:
   - **Rule Type** - Select one of the following:
     - **Table:** Captures either row changes resulting from DML changes or DDL changes to a particular table.
     - **Schema:** Captures either row changes resulting from DML changes or DDL changes to the database objects in a particular schema.
     - **Global:** Captures either all row changes resulting from DML changes or all DDL changes in the database.
   - **Statement Type** - Select **DDL**, **DML**, or **Both**.
   - **Secured Target Schema** - If you selected Table or Schema as the Rule Type, select the name of the schema to which the capture rule applies from the drop-down list.
   - **Secured Target Table** - If you selected Table as the Rule Type, select the name of the table to which the capture rule applies from the drop-down list.
7. Click **Save**.

   The capture rule is created and added to the list in the Capture Rule Settings page.

Understanding the Capture Rule Settings Page

Table 5–6 lists the columns used in the Capture Rule page.

Table 5–6 Columns in the Capture Rule Page

Column	Description
(Leftmost column)	A checkbox for selecting the audit setting
Problem icon	An exclamation mark icon indicates one of the following conditions: ▪ The setting is marked as needed in Oracle AVDF, but is not in use in the secured target database. ▪ The setting is in use at the secured target database, but is not marked as needed in Oracle AVDF.
Rule Type	The types of capture rules are as follows: ▪ **Table:** Captures or discards either row changes resulting from DML changes or DDL changes to a particular table. ▪ **Schema:** Captures or discards either row changes resulting from DML changes or DDL changes to the database objects in a particular schema. ▪ **Global:** Captures or discards either all row changes resulting from DML changes or all DDL changes in the database.

Table 5–6 (Cont.) Columns in the Capture Rule Page

Column	Description
In Use	The arrow points upward if the setting is active in the secured target and downward if it has not been provisioned or is not active.
Needed	The arrow points upward if the audit setting is marked as needed in Oracle AVDF, and downward if the audit setting is marked as not needed. If an audit setting that is not in use is set to needed, the **In Use** arrow points up after provisioning. If an audit setting that is in use is set to not needed, the audit setting is no longer displayed after provisioning.
Schema	Indicates the schema to which this rule applies
Table	For table capture rules, this fields indicates the table to which this rule applies.
Statement Type	Indicates the type of statements that are audited: `DDL`, `DML`, or `Both`

Provisioning Audit Policies to an Oracle Database

After you have updated and/or created the audit policies for a secured target Oracle Database, you can provision the audit policy changes to that database.

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

- Exporting Audit Settings to a SQL Script
- Provisioning the Audit Settings from the Audit Vault Server

> **Caution:** Any audit setting that is not indicated as **Needed** in the Audit Vault Server console will be turned off on the secured target. See "Specifying Which Audit Settings Are Needed" on page 5-3.

Exporting Audit Settings to a SQL Script

You can export audit policy settings for a secured target to a SQL script from Oracle AVDF. Then you can give the script to a database administrator for the secured target Oracle Database to use to update the audit settings on that database.

To export the audit settings to a SQL script for a secured target database:

1. Log in to the Audit Vault console as an auditor, and click the **Policy** tab.

   The Audit Settings page is displayed, showing the Oracle database secured targets to which you have access.

2. Click the name of a secured target database.

   The Audit Settings Overview for that database appears.

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

4. Click **Export/Provision**.

   The Export/Provision Audit Settings page appears, displaying the exportable audit commands.

5. Click **Export**, and then click **OK** to confirm.

6. Save the SQL file to a location on your system.
7. Give the saved script to the database administrator for that secured target. The database administrator can then apply the policies to the secured target. To verify that the settings have been updated, you can retrieve the audit settings as described in "Retrieving Audit Settings from an Oracle Database" on page 5-2.

Provisioning the Audit Settings from the Audit Vault Server

You can provision the audit policy settings directly from the Audit Vault Server to the secured target Oracle database. This updates the audit settings in the secured target without the intervention of a database administrator. However, a database administrator can modify or delete these audit settings, as well as add new ones. For this reason, you should periodically retrieve the settings to ensure that you have the latest audit settings. See "Retrieving Audit Settings from an Oracle Database" on page 5-2.

To provision the audit settings to the secured target:

1. Log in to the Audit Vault Server console as an auditor, and click the **Policy** tab.

   The Audit Settings page is displayed, showing the Oracle database secured targets to which you have access.
2. Click the name of a secured target database.

   The Audit Settings Overview for that database appears.
3. Select from the audit types you want to provision: **Statement**, **Object**, **Privilege**, **FGA**, or **Capture Rule**.
4. Click **Export/Provision**.

   The Export/Provision Audit Settings page appears, displaying the exportable audit commands, and allowing you to verify them before provisioning.
5. In the **Username** 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 secured target 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.
6. In the **Password** field, enter the password of this user.
7. Click **Provision**, and then click **OK** to confirm.

6

Generating Reports

Topics

Instructions for Generating and Customizing Reports

Report Descriptions

For descriptions of the Entitlement reports, see "Entitlement Report Descriptions" on page 7-4.

About the Reports in Audit Vault and Database Firewall

The Oracle AVDF reports are automatically generated reports that reflect audit data collected from secured targets, as well as data monitored by any Database Firewalls you have configured. You can save or schedule reports in either PDF or Excel format. You can also view reports online and interactively adjust the online report view by filtering data. You can save these interactive views to see them online later.

The reports are organized into various categories, such as access reports and management reports. An alerts report allows you to view and respond to alerts. You can also create user-defined reports that focus on specific audit events or firewall data.

You can also produce Sarbanes-Oxley (SOX), Payment Card Industry (PCI), Data Protection Act (DPA), Gramm-Leach-Bliley Act (GLBA), and Health Insurance Portability and Accountability Act (HIPAA) reports. To specify which of these reports are required for a secured target database, you can add the secured target to the appropriate group (such as the SOX group) from the **Secured Targets** tab. See "Creating and Modifying Secured Target Groups" on page 2-5.

Auditors can view data and modify reports for secured targets to which they have been granted access by a super auditor. However, an auditor can also send a report to other auditors for attestation regardless of the access rights of the other auditors.

You can specify email recipients for scheduled reports once they are generated, as well as create email templates for report notifications. See "Creating or Modifying an Email Template" on page 3-5.

Related Event Data Appendices

For audit data, reports track the audit events described in the following Appendices:

- Appendix C, "Oracle Database Audit Events" on page C-1
- Appendix D, "Sybase ASE Audit Events" on page D-1
- Appendix E, "Microsoft SQL Server SQL Trace Audit Events" on page E-1
- Appendix F, "Microsoft SQL Server SQL Audit and Event Log Events" on page F-1
- Appendix G, "IBM DB2 Audit Events" on page G-1
- Appendix H, "MySQL Audit Events" on page H-1
- Appendix I, "Solaris Operating System Audit Events" on page I-1
- Appendix J, "Microsoft Windows Operating System Audit Events" on page J-1
- Appendix K, "Linux Operating System Audit Events" on page K-1
- Appendix L, "Oracle ACFS Audit Events" on page L-1
- Appendix M, "Active Directory Audit Events" on page M-1

Browsing the Built-In Reports

From the Built-in Reports section of the **Reports** tab, you can browse report data online, schedule reports, and link to previously scheduled and generated reports.

To generate or browse the built-in reports:

1. Log in to the Audit Vault Server console as an auditor, and then click the **Reports** tab.
2. Click a link under the **Built-in Reports** menu (for example, Compliance Reports), navigate to the report you want, and do one of the following:
   - Click the **List generated reports** icon to view a previously scheduled and generated report. See Downloading Generated Reports in PDF or XLS Format
   - Click the **Browse report data** icon to view and browse the report data online. Timestamps in reports when you browse them online are displayed in your local browser time.
   - Click the **Schedule Report** icon to schedule the report in PDF or XLS format. See "Scheduling and Generating PDF or XLS Reports" on page 6-11. Timestamps in a PDF or XLS report are written in the Audit Vault Server time (based on the **Timezone Offset** setting specified by an administrator).
3. When browsing a report, click the Detail Page icon in the leftmost column for a row (an audit event) to view detailed information for that event.

   See "Audit Record Fields" on page B-1 for a description of each field in an audit record.

Downloading a Report in HTML or CSV Format

You can download reports you are browsing online as CSV (for use in an Excel spreadsheet) or HTML files.

To download a report in HTML or CSV format:

1. Log in to the Audit Vault Server console as an auditor, and access the report that you want.
2. From the **Actions** menu, select **Download**.
3. Select **CSV** or **HTML**.
4. In the File Download dialog box, click **Save**.
5. Click **Save As** dialog, select a location and enter a name for the file.
6. Click **Save**.

Customizing the Built-in Reports

Topics

About Customizing Built-in Reports

You can create customized reports based on the built-in reports and then save the new report formats. Oracle AVDF provides tools to filter, group, and highlight data, and define columns displayed in the reports. You can also create a categories for your saved reports. Customized and saved reports are listed on the **Interactive Reports** page.

While you can schedule the default built-in reports to be generated in PDF format, saved custom reports cannot be scheduled or printed in PDF format, and therefore must be viewed online.

Filtering and Controlling the Display of Data in a Report

Topics

About Filtering and Display Settings in Reports

You can control the display of data in a report to focus on a particular set of data. Oracle AVDF 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 as

a custom report (see "Saving your Customized Reports" on page 6-10).

Filtering Data in a Report

Topics

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.

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 the report 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.

Filtering Column and Row Data Using the Search Bar 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 all columns).

To search for row data in one or all columns:

1. Log in to the Audit Vault Server as an auditor, click the **Reports** tab, and access the report that you want.
2. If you want to focus the search on a specific column, in the Search bar, use the Search icon to select from the drop-down list of available columns.

   By default, the search applies to all columns.
3. In the Search bar text area, enter all or part of the row text you want to search for.
4. Click **Search**.

Filtering All Rows Based on Data from a Selected Column This filtering method lets you filter data in all rows based on a selected column (for example, all rows that contain `SYS` in the **User** column).

To filter all rows based on data from a selected column:

1. Log in to the Audit Vault Server as an auditor, click the **Reports** tab, and access the report that you want.
2. Click the **Actions** menu, and select **Filter**.

   The Filter dialog box appears. The existing filter definitions for the current user session are shown below the Filter dialog box.
3. For **Filter Type**, select **Column**.
4. In the **Column** drop-down list, select the column on which you want to base the filter.

   You can select from columns that are displayed in the report or other columns.
5. Click **Apply**.

The existing filter definitions for the current user session are shown above the report columns.

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

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, even those that are not shown in the current report.

To filter row data using an expression:

1. Log in to the Audit Vault Server as an auditor, click the **Reports** tab, and access the report that you want.
2. From the **Actions** menu, select **Filter**.

   The Filter dialog box appears. The existing filter definitions for the current user session are shown below the Filter dialog box.
3. For **Filter Type**, select **Row**.

   The Filter Expression fields appears along with Columns and Function/Operators fields to help you build the expression
4. Use the **Columns**, **Function/Operators**, and **Filter Expression** fields to build your filter expression:
   - **Columns:** Select the name(s) of the column(s) from the list to use them in the expression. When you select a column, its abbreviation appears in the Filter Expression field.
   - **Functions/Operators:** Select function(s) and/or operator(s) from the list to build your expression.
   - **Filter Expression:** If you have built an expression from the available columns, functions and operators, enter any parameters needed to complete your expression. If you type the expression, remember that it is case-sensitive. In most cases, use uppercase letters.
5. Click **Apply**.

   Oracle AVDF filters the display of row data based on the expression you created, and adds the filter definition above the report columns.
6. To enable or disable the display of the filtered data, select its corresponding check box. To remove a filter, click its **Remove Filter** icon.

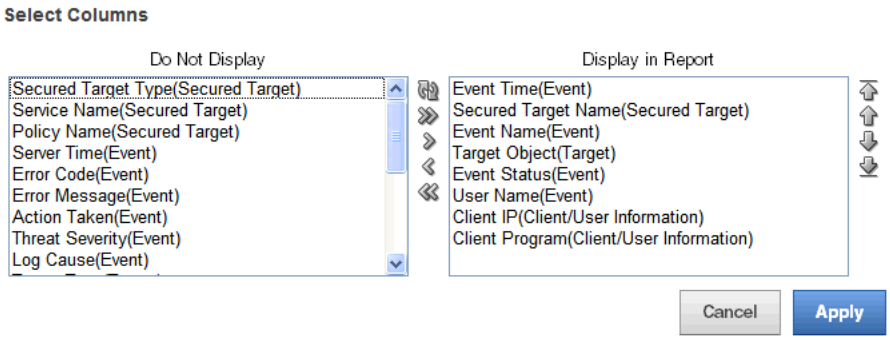
Hiding or Showing Columns in a Report

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.

To hide or show columns in a report:

1. Log in to the Audit Vault Server as an auditor, click the **Reports** tab, and access the report that you want.
2. From the **Actions** menu, click **Select Columns**.

   The Select Columns dialog field appears.



3. Move column names under the **Do Not Display** or **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.
4. To set the order of displayed columns, in the **Display in Report** box, select the column name, then click the up or down arrow on the right side of the box to reorder the column's position in the list.
5. Click **Apply**.

Formatting Data in a Report

Topics

- Sorting Row Data for All Columns
- Highlighting Rows in a Report
- Charting Data in a Report
- Adding Control Breaks to a Report

Sorting Row Data for All Columns To sort row data for all columns:

1. Access the report that you want.
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.
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**.

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.
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`.
5. Click **Apply**.

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.
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.

Adding Control Breaks to a Report You can create a break group based on selected column(s). This pulls the column(s) out of the report as a master record and groups all rows with the same value for the selected column under that master record. This is useful for filtering by multiple column values.

For example, you may have an Activity Overview report that displays several columns of data. If you want to see that data broken up by the Client IP Address and Secured Target Name columns, you would add control breaks for those columns. The resulting report would have data broken up into smaller tables for each unique combination of Client IP Address and Secured Target Name.

To add a control break in a column:

1. Access the report that you want.
2. From the **Actions** drop-down list, select **Format**, then select **Control Break**.
3. Select the column(s) to which you want to add a control break.

   You can select up to six columns in the order that you want the data to be broken up.

4. Click **Apply**.

Using the Group By Function to Format a Report The Group By dialog lets you group data by up to three columns in a report, and specify up to three functions to perform on any column, and display the resulting values as additional columns in the custom report.

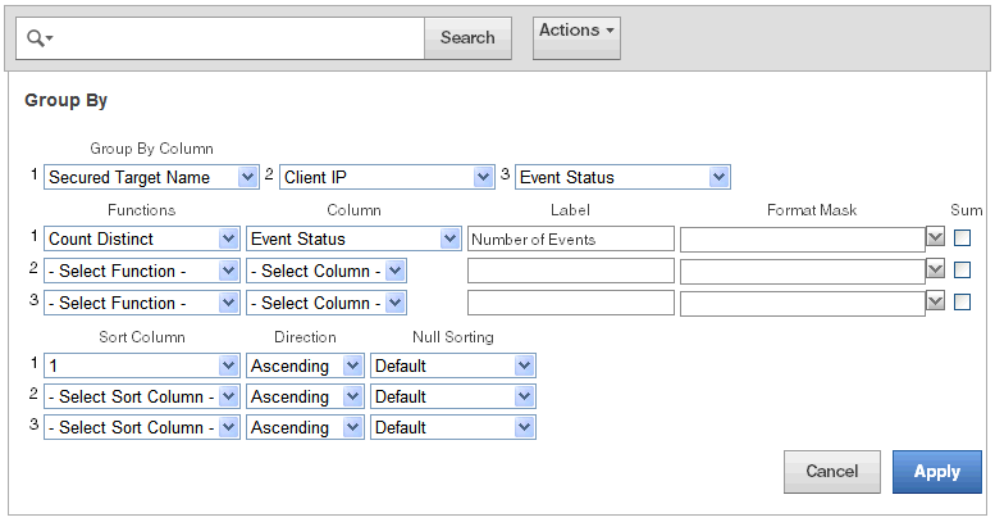
For example, suppose you want to create a custom report to show the number of events of a certain status (for example SUCCESS or FAILURE) for each secured target and client IP address combination. Using Group By, you can create a custom report to group unique secured targets together in the first column, client IP addresses for each secured target together in the second column, and display Event Status in the third column. You then specify a function to count distinct values in the Event Status column for each secured target and client IP address combination.

The resulting custom report will contain four columns: Secured Target, Client IP, Event Status, and the final column will show the results of the function, for example, the number of events with SUCCESS status for that secured target and IP address.

To use the Group By feature:

1. Access the report you want.
2. From the **Actions** drop-down list, select **Format**, then select **Group By**.

   The Group By dialog is displayed.



3. In the Group By Column section, from the first drop-down list, select a data column for grouping data in column 1 of your custom report.

   For example, if you select Secured Target Name, column 1 of your report will have secured targets grouped together. Optionally, select data groupings for columns 2 and 3 of your report.
4. Optionally, in the Functions section, specify up to three functions to operate on specific data columns:
   a. Under Functions, select a function, such as Count Distinct.
   b. Under Column, select any data column in the default report.
   c. Optionally, under Label, enter a column heading for the new column created by the result of this function.
   d. Optionally, under Format Mask, select the format of the data in the new column created by the result of this function.
   e. Optionally, select the **Sum** check box if you want to add a Sum row at the bottom of your custom report to add the values in the new column.
5. Optionally, in the sorting section, define the sort order for your custom report columns.
6. Click **Apply**.

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.
2. From the **Actions** menu, select **Reset**.

Saving your Customized Reports

When you customize a built-in report with your specified filters and display settings, you can save this customized report. Saved reports are listed in the **Interactive Reports** page in the **Reports** tab. The saved reports cannot be printed in PDF format, and therefore must be viewed online.

When you save a custom report, you can save it under a specific category that you select or create as you save the report. You can also make the custom report private or share it with other users as a public report.

To create and save a custom report starting from a built-in report:

1. Log in to the Audit Vault Server as an auditor, click the **Reports** tab, and access the report that you want.
2. Filter and design the display as needed.

   See "Filtering and Controlling the Display of Data in a Report" on page 6-3.
3. From the **Actions** menu, select **Save Report**.
4. Enter the following information in the Save Report dialog box:
   - **Name:** Enter a name for the report.
   - **Public:** Select this check box to make the report accessible to all users.
   - **Category:** Select from the list of available categories, or select **New Category**, then enter a name for the new category.

     When you save the report, the category appears in the **Category** column of the saved reports list.
   - **Description:** Enter a brief description of the report.
5. Click **Apply**.

   The custom report data is displayed, and the custom report is listed on the **Interactive Reports** page.

Accessing Your Saved Custom Reports

To access a saved custom report:

1. Log in to the Audit Vault Server as an auditor.
2. Click the **Reports** tab, and under **Custom Reports**, click **Interactive Reports**.

   The Saved Reports page appears.
3. In the **Report Name** column, select the link for the report that you want to access.

   The report appears. From here, you can:
   - Click the saved report name to edit it.
   - Click a filter to modify it
   - Enable or disable a filter by selecting or unselecting its check box
   - Remove a filter by clicking the Remove Filter icon (an "X")
   - Enable or disable a control break by selecting or unselecting its check box
   - Remove a control break by clicking the Remove Breaks icon (an "x")

   For information on changing the report settings, or disabling and enabling the report filters, see "Filtering Data in a Report" on page 6-4.

Scheduling and Generating PDF or XLS Reports

Topics

About Scheduling and Creating PDF or XLS Reports

You can schedule reports to be sent to other users in PDF or XLS format. You can run the report immediately, or you can create or select a schedule to run the report at a later time. You can specify a list of users who receive notifications of the report, or who need to attest to the report.

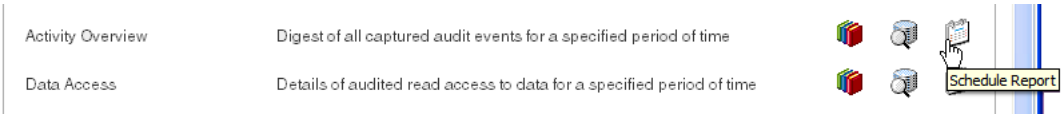
Note that interactive reports (saved reports you created by customizing built-in reports) cannot be scheduled.

Note: The timestamp shown in scheduled reports is based on the **Timezone Offset** setting specified by the administrator in the Audit Vault Server. See *Oracle Audit Vault and Database Firewall Administrator's Guide* for more information.

Creating a Report Schedule

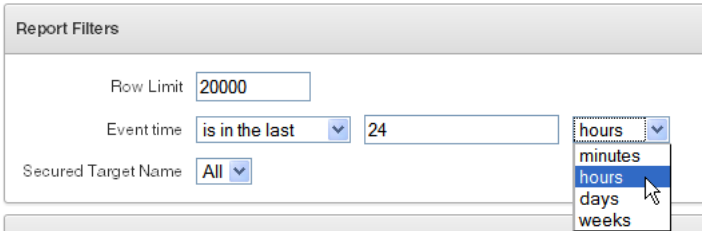
To schedule and create a PDF or XLS report:

1. Log in to the Audit Vault console as an auditor, and click the **Reports** tab.
2. Find the report you want to schedule, and click the schedule icon for the report.

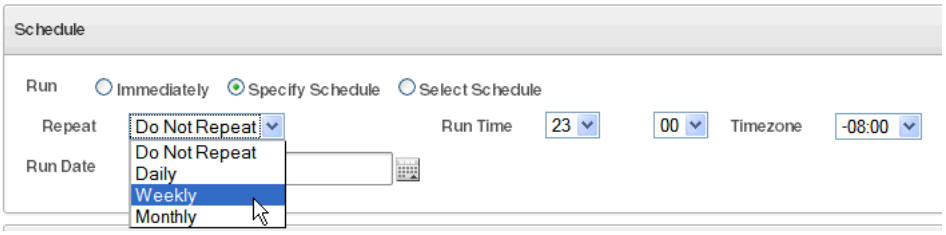


3. At the top of the Create/Edit Scheduled Job page, in the Schedule Report section, select the **Report Format** (**PDF** or **XLS**).

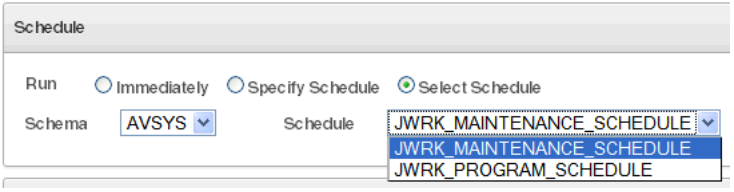
   You can optionally change the **Category Name** and **Report Name** fields.
4. In the Report Filters section, enter or select:
   - Row Limit
   - Event Time
   - Secured Target Name (or All) - This appears if applicable to the report.



5. In the Schedule section, select how you want to schedule the report:
   - **Immediately** - Run the report immediately
   - **Specify Schedule** - Select a run time, timezone, run date, and how often to repeat the schedule.



   - **Select Schedule** - (See Note) Select an existing schedule for the report by selecting a **Schema** where the schedule is stored, and the name of the **Schedule** from the drop-down lists.



     Note: This options only appears if a database administrator creates these schedules in the embedded Oracle Database using the `DBMS_SCHEDULER` PL/SQL 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, the **Schema** drop-down list contains the `SYS` schema, which owns the `DBMS_SCHEDULER` package.

6. In the Retention Policy section, if necessary, click **Change** to change the default archiving policy, and then click **Save**.

   The archiving (or retention) policy is created by an Oracle AVDF administrator, and determines how long the generated PDF or XLS report is retained in the Audit Vault Server before it is archived. If you do not select one, the default retention policy will be used (12 months retention online and 12 months in archives before purging). See *Oracle Audit Vault and Database Firewall Administrator's Guide* for more information on archiving policies.

7. In the Notification section, optionally select users to notify about this report, and then click **Add to List**:
   - For the **Send** field, select either **Notification** to send an email with a link to the report, or **Attachment** to send an email with the report attached as an XLS or PDF file.
   - From the **Template** drop-down list, select a report notification template.

- From the **Distribution List** drop-down list, if applicable, select a distribution list.
- If you want to send the report to additional recipients, enter their email addresses in the **To email** and **Cc** fields. Enter full email addresses separated by commas.

See also "Creating or Modifying an Email Distribution List" on page 3-5 and "Creating or Modifying an Email Distribution List" on page 3-5.

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. Click **Schedule**.

   The PDF or XLS is stored in the database, and the report appears in the **Report Schedules** page in the **Reports** tab.

   You can check the **Jobs** page in the **Settings** tab to see the status of report generation.

Viewing or Modifying Report Schedules

To view or modify report schedules, in the **Report Workflow** menu, click **Report Schedules**. To modify a report schedule, click the name of the report. See "Creating a Report Schedule" on page 6-11 for details on report schedule fields.

Downloading Generated Reports in PDF or XLS Format

When scheduled reports are generated you can download them to your computer in PDF or XLS format (depending on the format you selected in your report schedule). You can also notify other users by sending a link to the report, or attaching the report in an email.

You can download an unscheduled report in HTML or CSV format, while browsing it online. See "Downloading a Report in HTML or CSV Format" on page 6-3.

To list and download generated PDF or XLS reports you have scheduled:

1. Log in to the Audit Vault console as an auditor, and click the **Reports** tab.
2. Under **Report Workflow**, click **Generated Reports**.

   A list of generated reports appears.

3. From here, you can do the following:
   - To see a list of pending reports, click **Show Pending Reports**.
   - To save the report to your computer, click the report name, and then save the file.
   - To notify another user of the report, select the report, and then click **Notify**. See Notifying Users About Generated PDF or XML Reports.
   - To attest and annotate the report, click the Details icon in the second column. See "Annotating and Attesting Reports" on page 6-14 for instructions.

Notifying Users About Generated PDF or XML Reports

To send notifications to other users or distribution lists about a scheduled and generated report:

1. Log in to the Audit Vault console as an auditor, and click the **Reports** tab.
2. Under **Report Workflow**, click **Generated Reports**.

   A list of generated reports appears.
3. Select the report you want and click the **Notify**.
4. Fill the fields as follows:
   - For the **Send** field, select either **Notification** to send an email with a link to the report, or **Attachment** to send an email with the report attached as an XLS or PDF file.
   - From the **Template** drop-down list, select a report notification template.
   - From the **Distribution List** drop-down list, if applicable, select a distribution list.
   - If you want to send the report to additional recipients, enter their email addresses in the **To email** and **Cc** fields. Enter full email addresses separated by commas.
5. Click **Notify**.

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.

To annotate and attest to a report:

1. Log in to the Audit Vault Server console as an auditor.

   The Dashboard page appears.
2. Access the list of reports to attest to by doing one of the following:
   - From the **Home** page, under **Attestation Actions**, select the report from the list.
   - Click the **Reports** tab, and under the **Report Workflow** menu, select **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 "Filtering Data in a Report" on page 6-4 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.

Creating and Uploading Your Own Custom Reports

You can add your own custom reports by using Oracle BI Publisher, or another report authoring tool from a third party. You will need a report definition file (XML format) and a report template (RTF format), which you can download from Oracle AVDF. This section describes how to download these files from an existing Oracle AVDF report and use them for your own report.

The audit event appendices in this guide contain data that may help you in creating your own reports. See "Related Event Data Appendices" on page 6-2.

To add a report starting from an existing report definition and template file:

1. Log in to the Audit Vault Server console as an auditor.
2. Click the **Reports** tab, and under **Custom Reports**, click **Uploaded Reports**.

   The Uploaded Reports page is displayed, listing any previously uploaded custom reports, and built-in reports in the Pre-configured Reports section.
3. Find a pre-configured report to use as a starting point for your new custom report.
4. Download the report definition and template files for the report you want:
   a. Click the **Download Report Template** icon and save the RTF file.
   b. Click the **Download Report Definition** icon and save the XML file.
5. Customize the report definition and template files using either Oracle BI Publisher or another tool, as necessary.

   Refer to Oracle BI Publisher documentation available from this page: `http://www.oracle.com/technetwork/documentation/index.html`.
6. Click **Upload**.
7. In the **Report Template file** field, enter the name or browse for your customized report template (RTF) file.
8. In the **Report Definition file** field, enter the name or browse for your customized report definition (XML) file.
9. Click **Save**.

   The new report is listed under Uploaded Reports.

Audit Report Descriptions

Topics

About the Audit Reports

You can access Audit Reports from the **Reports** tab by clicking **Audit Reports**. There are four groups of Audit Reports:

- Activity Reports
- Alert Reports
- Entitlement Reports (see "Managing and Viewing Entitlement Data" on page 7-1)
- Stored Procedure Audit Reports

This section contains information about Activity, Alert, and Stored Procedure Reports.

Activity Reports

Topics

About the Activity Reports

You can access Activity Reports from the **Reports** tab by clicking **Audit Reports**.

The default activity reports track general database access activities such as audited SQL statements, application access activities, and user login activities. These reports display the following kinds of information: secured target name, secured target type, host name for the secured target, version of the secured target, IP address of the secured target, audit time, 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.

Activity Overview Report

The **Activity Overview** page displays information about all monitored and audited events. Events 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 Oracle AVDF 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 Oracle AVDF administrator to check the server-side log files (alert and trace logs) for errors. If there are errors, then contact Oracle Support.

Data Access Report

The Data Access Report displays audited read access to data for a specified period of time.

> **See Also:** "Related Event Data Appendices" on page 6-2 for related data access audit events in a specific secured target type

Data Modification Report

The Data Modification Report displays the details of audited data modifications for a specified period of time.

Data Modification Before-After Values

The Data Modification Before-After Values Report displays details of audited data modifications for a specified period of time, showing before and after values.

Data for this report comes from the TRANSACTION LOG audit trails written by databases. Be sure that an Oracle AVDF administrator has configured and started a TRANSACTION LOG audit trail for the secured target you want to monitor. This report then pulls data from database transaction (redo) logs.

Database Schema Changes Report

The Database Schema Changes Report displays details of audited DDL activity for a specified period of time.

All Activity Report

The All Activity Report displays details of all captured audit events for a specified period of time.

Failed Logins Report

The Failed Logins Report displays details of audited failed user logins for a specified period of time.

User Login and Logout Report

The User Login and Logout Report displays details of audited successful user logins and logouts for a specified period of time.

Entitlements Changes Report

The Entitlements Changes Report displays details of audited entitlement related activity for a specified period of time.

Audit Settings Changes Report

The Audit Settings Changes Report displays details of observed user activity targeting audit settings for a specified period of time.

Secured Targets Startup/Shutdown Report

The Secured Targets Startup/Shutdown Report displays details of observed startup and shutdown events for a specified period of time.

Alert Reports

Alert reports are accessed from the **Reports** tab, by clicking **Audit Reports**.

The alert reports track critical and warning alerts. An alert is raised when data in audit records matches a predefined alert rule condition. Alerts are grouped by associated secured target, by event category, and by the severity level of the alert (either warning or critical).

There are three alert reports:

- **All Alerts Report** - This report shows all alerts, both critical and warning alerts, issued within a specified period of time.
- **Critical Alerts Report** - This report shows critical alerts issued within a specified period of time.
- **Warning Alerts Report** - This report shows warning alerts issued within a specified period of time.

See Also:

- "Creating and Configuring Alerts" on page 8-1 for information about creating and configuring alerts
- "Responding to an Alert" on page 8-7 for information about responding to an alert

Stored Procedure Auditing Reports

You can access Stored Procedure Auditing reports from the **Reports** tab by clicking **Audit Reports**.

Stored procedure auditing reports allow you to audit changes to stored procedures on secured target databases. Oracle AVDF connects to the secured target database at scheduled intervals and discovers any changes or additions that have been made to stored procedures.

Table 6–1 lists the Stored Procedure Auditing reports.

Table 6–1 Stored Procedure Auditing Reports

Report	Description
Stored Procedure Activity Overview	Digest of all audited operations on stored procedures for a specified period of time
Stored Procedure Modification History	Details of audited stored procedure modifications for a specified period of time
Created Stored Procedures	Stored procedures created within a specified period of time
Deleted Stored Procedures	Stored procedures deleted within a specified period of time
New Stored Procedures	Latest state of stored procedures created within a specified period of time

Compliance Report Descriptions

Topics

- About the Compliance Reports
- Associating Secured Targets with Compliance Report Categories
- Reports Included in Each Compliance Report Category

About the Compliance Reports

The compliance reports provide out-of-the-box reports to help you meet regulations associated with credit card, financial, data protection, 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.

The following compliance report categories are available:

- Payment Card Industry (PCI) Reports
- Gramm-Leach-Bliley Act (GLBA) Reports
- Health Insurance Portability and Accountability Act (HIPAA) Reports
- Sarbanes-Oxley Act (SOX) Reports
- Data Protection Act (DPA) Reports

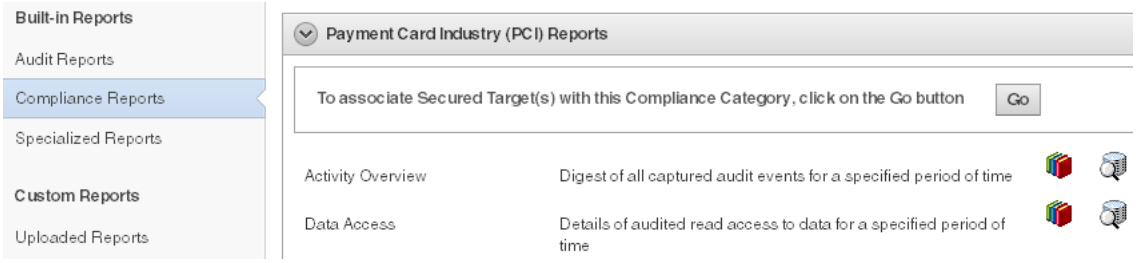
To access the compliance reports, click the **Reports** tab, then from the **Built-in Reports** menu, select **Compliance Reports**.

Associating Secured Targets with Compliance Report Categories

In order to generate compliance reports for a secured target, you must add it to a compliance report category.

To associate secured targets with compliance report categories from the Compliance Reports page, click the **Go** button for a compliance category, as shown in Figure 6–1.

Figure 6–1 Associating Secured Targets With Compliance Report Categories



This takes you to the **Groups** page under the **Secured Targets** tab, and allows you to add a secured target as a member of a compliance group in Oracle AVDF. See "Managing Compliance for Secured Target Databases" on page 2-6 for detailed instructions on assigning secured targets to compliance groups.

Reports Included in Each Compliance Report Category

Table 6–2 lists the set of reports available for each compliance report category.

Table 6–2 Compliance Reports Included for each Compliance Category

Report Name	Description
Activity Overview	Digest of all captured audit events for a specified period of time
Data Access	Details of audited read access to data for a specified period of time

Table 6–2 (Cont.) Compliance Reports Included for each Compliance Category

Report Name	Description
Data Modification	Details of audited data modifications for a specified period of time
Database Schema Changes	Details of audited DDL activity for a specified period of time
All Activity	Details of all captured audit events for a specified period of time
Failed Logins	Details of audited failed user logins for a specified period of time
User Login and Logout	Details of audited successful user logins and logouts for a specified period of time
Entitlements Changes	Details of audited entitlement related activity for a specified period of time
Audit Settings Changes	Details of observed user activity targeting audit settings for a specified period of time
Secured Target Startup/Shutdown	Details of observed startup and shutdown events for a specified period of time
Stored Procedure Activity Overview	Digest of all audited operations on stored procedures for a specified period of time
Stored Procedure Modification History	Details of audited stored procedure modifications for a specified period of time
Created Stored Procedures	Stored procedures created within a specified period of time
Deleted Stored Procedures	Stored procedures deleted within a specified period of time
New Stored Procedures	Latest state of stored procedures created within a specified period of time

Specialized Database Firewall Report Descriptions

Topics

About the Specialized Database Firewall Reports

Database Firewall reports contain data that is collected if a secured target is monitored by the Database Firewall according to a firewall policy, as well as data gathered if Oracle AVDF is integrated with BIG-IP ASM Web application firewall (WAF) from F5 Networks, Inc.

Data collected by the Database Firewall includes:

- Database Firewall action and threat level
- Database user name
- OS user name
- Statement type (data definition, procedural, data manipulation, etc.)
- Client application name and IP address
- SQL request ID

- Database Firewall cluster ID
- Comparison data between F5's WAF policy and the Database Firewall policy

To access these specialized reports, click the **Reports** tab, then from the **Built-in Reports** menu, select **Specialized Reports**.

Database Firewall Policy Reports

Table 6–3 lists the Database Firewall Policy reports.

Table 6–3 Database Firewall Policy Reports

Report Name	Description
Database traffic analysis by client IP detail	Audit details for statements grouped by protected database and client IP address
Database traffic analysis by OS user detail	Audit details for statements grouped by protected database and OS user
Database Traffic Analysis by User Blocked Statements	Audit details for blocked statements grouped by protected database and OS user
Database Traffic Analysis by User Warned Statements	Audit details for warned statements grouped by protected database and OS user
Database Traffic Analysis by User Invalid Statements	Audit details for invalid statements grouped by protected database and OS user

Database Firewall F5 Reports

Table 6–4 lists the specialized Database Firewall F5 reports.

Table 6–4 Database Firewall F5 Reports

Report Name	Description
F5 Confirmed Alert	F5 alerts confirmed as Out of Policy by the Database Firewall policy
F5 Incident Report	F5 incidents by time
F5 No WAF match	Alerts from F5's Web Application Firewall (WAF) not matched by any SQL traffic
F5 Policy Conflict by User	F5 alerts raised, but confirmed as In Policy by the Database Firewall policy, for each user
F5 Policy Conflict	F5 alerts raised, but confirmed as In Policy by the Database Firewall policy
F5 WAF Blocked Alert	Alerts blocked by F5

7

Managing Entitlements

Topics

Managing and Viewing Entitlement Data

Oracle AVDF provides a set of default entitlement reports and allows you to retrieve entitlement data from Oracle Database secured targets. In addition, you can create snapshots of entitlement data at specific points in time, and group them under labels that you specify, in order to compare them in the reports.

You can filter a report to show the data from an earlier snapshot or label, or you can compare the entitlement data from two snapshots or two labels. For example, you can find how user privileges have been modified between two snapshots or labels.

> **Note:** For Oracle Database 12*c* secured targets, if you are not using multitenant container databases (CDBs), entitlement data appears as for earlier versions of Oracle Database. If you are using CDBs, each pluggable database (PDB) or CDB is configured as a separate secured target in the Audit Vault Server, and entitlement data appears accordingly in snapshots and reports.

The general steps for managing and viewing entitlement data are:

1. Retrieve the entitlement data from the secured target to create a snapshot of the data at that point in time. See:
   - "Retrieving User Entitlement Data for Oracle Database Secured Targets" on page 2-4
2. Optionally, create labels to organize the entitlement snapshots into meaningful groups, and assign the labels to snapshots. See:
   - "Creating, Modifying, or Deleting Labels for Entitlement Snapshots" on page 7-2
   - "Assigning Labels to Entitlement Snapshots" on page 7-3
3. View entitlement reports, using snapshots and labels to filter and compare data. See:

Working With Entitlement Snapshots and Labels

Topics

About Entitlement Snapshots and Labels

When you retrieve entitlement data from an Oracle Database secured target, a **snapshot** of that data is created, and added to the list in the User Entitlement Snapshots page in the **Secured Targets** tab. See "Retrieving User Entitlement Data for Oracle Database Secured Targets" on page 2-4.

An entitlement snapshot captures the state of user entitlement information at a specific point in time. The snapshot contains the metadata of users and roles that a user has to that Oracle Database: system and other SQL privileges, object privileges, role privileges, and user profiles. You can only view and manage snapshots for secured targets to which you have access.

Each snapshot is unique for a secured target. The name for a snapshot is the time stamp assigned to it when the entitlement data was retrieved, for example, `9/22/2009 07:56:17 AM`. If you retrieve entitlement data for all your secured targets at this time, then each secured target has its own `9/22/2012 07:56:17 AM` snapshot.

Labels allow you to organize snapshots into meaningful categories so that you can view and compare groups of snapshots together. For example, suppose the secured targets `payroll`, `sales`, and `hr` each have a `9/22/2012 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 entitlement data at that time from the three secured targets, together in the same report.

Creating, Modifying, or Deleting Labels for Entitlement Snapshots

To create or delete a label:

1. Log into the Audit Vault Server console as an auditor, and click the **Secured Targets** tab.
2. From the **Entitlement Snapshots** menu on the left, click **Manage Labels**.
3. From this page:
   - To create a label, click **Create**, enter a name and an optional description, and then click **Save**.
   - To delete a label, select the label, and then click **Delete**.
   - To edit the name or description of a label, click the name of the label, make your changes, and then click **Save**.

Assigning Labels to Entitlement Snapshots

Before you can assign labels to snapshots, you must first retrieve entitlement data from an Oracle Database secured target, which creates a snapshot each time you do so. See "Retrieving User Entitlement Data for Oracle Database Secured Targets" on page 2-4 for instructions.

To assign labels to entitlement snapshots:

1. Log into the Audit Vault Server console as an auditor, and click the **Secured Targets** tab.
2. From the **Entitlement Snapshots** menu on the left, click **Manage Snapshots**.

   A list of snapshots of user entitlement data appears along with the timestamp for when the data was collected and the label assigned to the snapshot, if any.

   You can adjust the appearance of the list from the **Actions** menu. See "Working with Lists of Objects in the UI" on page 1-12.
3. To assign a label to snapshots:
   a. Select the snapshots, and click **Assign Label**.
   b. Select a **Label** from the drop-down list.
   c. Optionally, enter a description.
   d. Click **Save**.
4. To delete a snapshot, select the snapshot, and then click **Delete**.

Generating Entitlement Reports

Topics

About Viewing Entitlement Reports with Snapshots and Labels

You can use snapshots and labels to filter and compare entitlement data in reports. After snapshots have been created, and you have optionally created and assigned labels to them, then you are ready to check the entitlement reports.

The type of entitlement report determines whether you can view its entitlement data by snapshot or by label. Reports that show data by secured target (for example, User Accounts by Secured Target) let you view and compare snapshots for a specific secured target. The other entitlement reports (such as User Accounts) let you view and compare entitlement data by label across all the secured targets.

Viewing Entitlement Reports by Snapshot or Label

To check entitlement reports for an individual snapshot or label:

1. Log in to the Audit Vault Server console as an auditor.
2. Click the **Reports** tab, and in the Audit Reports page, expand **Entitlement Reports**.
3. Click the **Browse report data** icon for the entitlement report that you want.

4. In the entitlement report, do the following:
   - If the report is "by secured target," select a secured target.
   - From the **Snapshot** or **Label** list, select the snapshot or label.
5. Click **Go**.

   The entitlement report data appears. The generated report contains a 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. See "Filtering Data in a Report" on page 6-4.
6. Optionally, you can save the report. See "Saving your Customized Reports" on page 6-10.

Comparing Entitlement Data Using Snapshots or Labels

To compare the entitlement data for two snapshots or labels:

1. Log in to the Audit Vault Server console as an auditor.
2. Click the **Reports** tab, and in the Audit Reports page, expand **Entitlement Reports**.
3. Click the **Browse report data** icon for the entitlement report that you want.
4. In the report, do the following:
   - If the report is "by secured target," select a secured target.
   - From the **Snapshot** or **Label** list, select the first snapshot or label.
   - Click the **compare** check box.
   - Select another snapshot or label from the second drop-down list for comparison.
5. Click **Go**.

The entitlement report data appears and the name of the report is appended with **Changes**. 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.

Entitlement Report Descriptions

Topics

About the Entitlement Reports

An entitlement report describes the types of access that users have to an Oracle database secured target. It provides information about the user, role, profile, and privileges used in the secured target.

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 "Generating Entitlement Reports" on page 7-3.

See Also:

- "Generating Entitlement Reports" on page 7-3 for information about generating and viewing entitlement report data
- "Filtering and Controlling the Display of Data in a Report" on page 6-3 and "Customizing the Built-in Reports" on page 6-3 for information about creating user-defined reports from entitlement reports

User Accounts Reports

The User Accounts Report and User Accounts by Secured Target Report show the following information about user accounts: secured target 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).

In Oracle AVDF 12.1.2: You can select these additional columns relating to Oracle 12c secured targets:

- Edition Enabled: Whether editions are enabled for this user
- Authentication Type: Authentication mechanism for this user
- Proxy Only Connect: Whether this user can connect only through a proxy
- Common: Whether this user is common to the PDB and CDB. **Y** indicates a common user, **N** indicates the user is local to the PDB, and null indicates the database is neither a PDB nor a CDB.
- Last Login: Last login timestamp for this user
- Oracle Maintained: Whether the user was created, and is maintained, by Oracle Database-supplied scripts. A **Y** value means this user must not be changed in any way except by running an Oracle Database-supplied script.
- Container: Container name. This is null if the database is not a PDB or CDB.

User Privileges Reports

The User Privileges Report and User Privileges by Secured Target Report show the following information about user privileges: secured target 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.

In Oracle AVDF 12.1.2: You can select these additional columns relating to Oracle 12c secured targets:

- Hierarchy: Privilege is with hierarchy option
- Type: Object type (table, view, sequence, etc.)
- Common: Whether this user is common to the PDB and CDB. **Y** indicates a common user, **N** indicates the user is local to the PDB, and null indicates the database is neither a PDB nor a CDB.
- Container: Container name. This is null if the database is not a PDB or CDB.

User Profiles Reports

The User Profiles Report and User Profiles by Secured Target Report show the following information about user profiles: secured target in which the user profile was created, profile name, resource name, resource type (KERNEL, PASSWORD, or INVALID), and profile limit.

In Oracle AVDF 12.1.2: You can select these additional columns relating to Oracle 12c secured targets:

- Common: Whether this user is common to the PDB and CDB. **Y** indicates a common user, **N** indicates the user is local to the PDB, and null indicates the database is neither a PDB nor a CDB.
- Container: Container name. This is null if the database is not a PDB or CDB.

Database Roles Reports

The Database Roles Report and Database Roles by Secured Target 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.

In Oracle AVDF 12.1.2: You can select these additional columns relating to Oracle 12c secured targets:

- Oracle Maintained: Whether the user was created, and is maintained, by Oracle Database-supplied scripts. A **Y** value means this user must not be changed in any way except by running an Oracle Database-supplied script.
- Common: Whether this user is common to the PDB and CDB. **Y** indicates a common user, **N** indicates the user is local to the PDB, and null indicates the database is neither a PDB nor a CDB.
- Container: Container name. This is null if the database is not a PDB or CDB.

System Privileges Reports

The System Privileges Report and System Privileges by Secured Target Report show the following information about system privileges: secured target 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.

In Oracle AVDF 12.1.2: You can select these additional columns relating to Oracle 12c secured targets:

- Common: Whether this user is common to the PDB and CDB. **Y** indicates a common user, **N** indicates the user is local to the PDB, and null indicates the database is neither a PDB nor a CDB.
- Container: Container name. This is null if the database is not a PDB or CDB.

Object Privileges Reports

The Object Privileges Report and Object Privileges by Secured Target Report show the following information about object privileges: the secured target 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.

In Oracle AVDF 12.1.2: You can select these additional columns relating to Oracle 12c secured targets:

- Hierarchy: Privilege is with hierarchy option
- Type: Object type (table, view, sequence, etc.)
- Common: Whether this user is common to the PDB and CDB. **Y** indicates a common user, **N** indicates the user is local to the PDB, and null indicates the database is neither a PDB nor a CDB.
- Container: Container name. This is null if the database is not a PDB or CDB.

Privileged Users Reports

The Privileged Users and Privileged Users by Secured Target reports show the following information about privileged users: secured target 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.

For Oracle Database versions prior to 12c, privileged users are identified by these roles:

```
SYSDBA
SYSOPER
```

For Oracle Database version 12c, the above two roles identify privileged users, in addition to the following roles:

```
SYSASM
SYSBACKUP
SYSDG
SYSKM
```

In Oracle AVDF 12.1.2: You can select these additional columns relating to Oracle 12c secured targets:

- Common: Whether this user is common to the PDB and CDB. **Y** indicates a common user, **N** indicates the user is local to the PDB, and null indicates the database is neither a PDB nor a CDB.
- Container: Container name. This is null if the database is not a PDB or CDB.

8

Creating Alerts

Topics

About Alerts

You can create and configure alerts on events for secured targets, and for third-party plug-ins that have been developed using the Oracle AVDF SDK. These events may be collected by the Audit Vault Agent or the Database Firewall. Alerts are independent of audit policies or firewall policies.

Alerts are rule-based. That is, if the rule definition is matched (for example, User A fails to log in to Client Host B after three tries), then an alert is raised. An alert can be applied to multiple secured targets, such as four Oracle databases. In this case, the rule can include more than one event and the event comes from different secured targets. For example, User A failed to log in to secured target X and User A also failed to log in to secured target Y.

You can specify an alert severity and associate the alert with the audit events described in Appendix C through Appendix G. Also, if a secured target is monitored by a Database Firewall, you can configure alerts based on audit records sent by the firewall, in addition to the alerts specified in the firewall policy (see "Creating Database Firewall Policies" on page 4-1.)

When you configure an alert, you can set up an email to be automatically sent to a user, such as a security officer, or to a distribution list. You can also configure templates to be used for email alert notification.

Alerts are raised when the audit data reaches the Audit Vault Server, not when the event that raises the alert occurs. The time lag between when the event occurs and when the alert is raised depends on several factors, including how frequently the audit trails are retrieved. The timestamp of an alert *event* indicates the time that the event occurred (for example, the time that User A tries to log in). The timestamp for the alert indicates when the alert was raised.

Creating and Configuring Alerts

Topics

Creating Alert Status Values

You can create alert status values to assign to an alert during the lifetime of the alert. Oracle AVDF 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 Server console as an auditor, then click the **Policy** tab.
2. From the menu on the left, click **Alerts**, then click **Manage Alert Status Values**.

   The Alert Status Values page appears. From here you can edit or delete existing user-defined alert status values.
3. To create a new alert status, click **Create**.
4. In the Create Alert Status Value page, 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.
5. Click **Save**.

   The new alert status appears in the Alert Status Values page.

Creating or Modifying an Alert

When you create an alert in Oracle AVDF, you define the conditions that will trigger the alert, and specify the type of notification that will be sent, and to whom. For example, you could create an alert that is raised each time User X tries to modify Table Y, and which will notify administrator Z, using a specific email notification template.

Oracle AVDF has a preconfigured alert that is triggered based on alert settings in your Database Firewall policy. The alerts you create are for audit and other events not associated with Database Firewall.

To create an alert:

1. Log in to the Audit Vault Server console as an auditor, and click the **Policy** tab.
2. From the menu on the left, click **Alerts**.

   The Alerts page appears, which lists the existing alerts. To view or modify the definition for an existing alert, click its name in the **Alert Name** field.

   You can adjust the appearance of the list from the **Actions** menu. See "Working with Lists of Objects in the UI" on page 1-12.
3. For a new alert click **Create**, otherwise, click the name of the alert to modify.

   The Create (or Modify) Alert page appears.
4. Enter the alert **Name** and optional **Description** in the appropriate fields.
5. Specify the following information:

- **Alert Severity:** Select **Warning** or **Critical**.
- **Secured Target Type:** Select secured target type, for example, Oracle Database.
- **Threshold:** Enter the number of times the alert condition should be matched before the alert is raised.
- **Duration:** If you entered a threshold value that is more than 1, enter the length of time (in minutes) that this alert condition should be evaluated to meet that threshold value. For example if you enter a threshold of 3 and duration of 5, then the condition must be matched 3 times in 5 minutes to raise an alert.
- **Group By:** Select a field from the list to group events by this column for this alert rule.
- **Condition:** Enter a Boolean condition that must be met for this alert to be triggered. The **Condition - Available Fields** area on the right lists the permissible fields you can use to build your condition in the following format:

  ```
  :condition_field operator expression
  ```

  You can use any valid SQL `WHERE` clause with the available fields, for example, your condition may be:

  ```
  upper(:EVENT_STATUS) = 'FAILURE'
  ```

  See "Defining Alert Conditions" on page 8-3 for details.

6. Optionally, in the **Notification** area:
   a. Specify the following information:
      - **Template:** Select a notification template to use for this alert.
      - **Distribution List:** Select an email distribution list that will be notified about this alert.
      - **To:** Enter email addresses, separated by commas, to receive notifications.
      - **Cc:** Enter email addresses, separated by commas, to be copied on notifications.

   b. Click **Add to List** to record the email recipients that you entered in the **To** and **Cc** fields.

   See also, "Creating Templates and Distribution Lists for Email Notifications" on page 3-4.

7. Click **Save**.

   The new alert appears in the Alerts page.

You can monitor alert activity from the dashboard on the Audit Vault Server console **Home** page. See "Monitoring Alerts" on page 8-6 for more information.

Defining Alert Conditions

Topics

About Alert Conditions

In the **Condition** field of the Create Audit Alert Rule page, you can construct a Boolean condition that evaluates audit events. When the Boolean condition evaluates to `TRUE`, then Oracle AVDF raises the alert, and notifies any specified users. 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:

```
:condition_field operator expression
```

Creating an Alert Condition

The Create Audit Alert Rule page contains available fields from an Oracle AVDF audit record that you can cut and paste to build your alert conditions. Table 8–1 describes the available fields for alert conditions.

Table 8–1 Available Fields for Alert Conditions

Condition Field	Description
ACTION_TAKEN	(Firewall Alerts) Action taken by the Database Firewall, for example: `BLOCK`, `WARN`, or `PASS`
AV_TIME	The time Oracle AVDF raised the alert
CLIENT_HOST_NAME	The host name of the client application that was the source of the event causing the alert
CLIENT_IP	The IP address of the client application that was the source of the event causing the alert

CLUSTER_TYPE	(Firewall Alerts) The cluster type of the SQL statement causing the alert. Values may be:
	`Data Manipulation`
	`Data Definition`
	`Data Control`
	`Procedural`
	`Transaction`
	`Composite`
	`Composite with Transaction`

COMMAND_CLASS	The Oracle AVDF command class. See Appendix C through Appendix M for details.
ERROR_CODE	The secured target's error code
ERROR_MESSAGE	The secured target's error message
EVENT_NAME	The secured target's audit event name. See Appendix C through Appendix M for details.
EVENT_STATUS	Status of the event: `Success` or `Failure`
EVENT_TIME	The time that the event occurred
NETWORK_CONNECTION	Description of the connection between the secured target database and the database client, in the following format: *`client_ip:client_port,database_ip:database_port`* For example: `198.51.100.1:5760,203.0.113.1:1521`
OSUSER_NAME	Name of the secured target's OS user
SECURED_TARGET_NAME	Name of the secured target in Oracle AVDF

Table 8–1 (Cont.) Available Fields for Alert Conditions

Condition Field	Description
TARGET_OBJECT	Name of the object on the secured target, for example, a table name, file name, or a directory name. Must be in upper case, for example, `ALERT_TABLE`.
TARGET_OWNER	Owner of the object on the secured target
TARGET_TYPE	The object type on the secured target, for example, `TABLE`, or `DIRECTORY`
THREAT_SEVERITY	(Firewall Alerts) The threat severity of the SQL statement triggering the alert, as defined in a Database Firewall policy. Values may be: `Unassigned`, `Insignificant`, `Minor`, `Moderate`, `Major`, or `Catastrophic`.
USER_NAME	User name of the secured target user

The above fields must be preceded by a colon (for example `:USER_NAME`) when used in the condition. Using these fields, you can build your condition as described below.

Use Any Legal SQL Function

You can use any legal SQL function, including user-defined functions. However, you cannot use sub-query statements. For example:

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

Use Any Legal SQL Operator

For example, you can use:

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

When using operators, follow these guidelines:

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

Use Wildcards

You can use the following wildcards:

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

Group Components of a Condition

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

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

Example of an Alert Condition

Suppose you want 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`.

To write a condition for this alert, you can copy the EVENT_NAME and USER_NAME fields from the available fields list, and use them to write this condition:

```
:EVENT_NAME='LOGON' and :USER_NAME='apps' and :CLIENT_IP=NULL
```

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

You can look up audit event names and attributes in Appendix C through Appendix G.

Forwarding Alerts to Syslog (AVDF 12.1.2)

This feature is available as of Oracle AVDF version 12.1.2.

In addition to seeing alerts in reports, and receiving them in notifications as specified in the alert configuration, you can also forward all alert messages to syslog.

As a prerequisite to forwarding alerts to syslog, the Oracle AVDF administrator must configure syslog destinations in the Audit Vault Server, and select **Alert** as a syslog category. See the *Oracle Audit Vault and Database Firewall Administrator's Guide* for instructions.

To forward all alerts to syslog:

1. Log in to the Audit Vault Server console as a super auditor.
2. Click the **Policy** tab.
3. Click **Alerts** from the menu on the left, and then click **Forward Alerts to Syslog**.

   All defined alerts are forwarded to syslog.

AVDF Syslog Alert Message Format

AVDF alerts appear in syslog in the following format:

```
[AVDFAlert@111 name="alert_name" severity="alert_severity"
url="auditor_console_URL_for_alert" time="alert_generated_time" target="secured_
target" user="username" desc="alert_description"]
```

The `user` and `target` parameters may list zero or more users or targets related to this alert.

Example:

```
Apr 16 23:22:31 avs08002707d652 logger: [AVDFAlert@111 name="w_1"
severity="Warning" url="https://192.0.2.10/console/f?p=7700..."
time="2014-04-16T22:55:30.462332Z" target="cpc_itself" user="JDOE" desc=" "]
```

Monitoring Alerts

Oracle AVDF raises an alert when data in a single audit record matches an alert rule condition. Auditors can view recently raised alerts in the dashboard on the Audit Vault Server console's **Home** page. Alerts are grouped by the time that the alerts are

raised, and by the severity level of the alert (warning or critical). From here, you can drill down to reports.

You can also schedule alert reports from the Audit Vault Server **Reports** tab. For details, see:

- "Alert Reports" on page 6-17
- "Scheduling and Generating PDF or XLS Reports" on page 6-11

Disabling, Enabling, or Deleting Alerts

You can disable an alert while keeping the alert definition in case you wish to enable this alert again in the future.

To disable or enable alerts:

1. Log into the Audit Vault Server console as an auditor, and click the **Policy** tab.
2. Click **Alerts** from the menu on the left.

   The alerts list is displayed. You can adjust the appearance of the list from the **Actions** menu. See "Working with Lists of Objects in the UI" on page 1-12.
3. Select the alerts you want, and then click **Disable**, **Enable**, or **Delete**.

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), or notify other users of the alert.

To respond to an alert:

1. Log in to the Audit Vault Server console as an auditor.
2. Access the alert by using one of the following methods:
   - From the Dashboard page, select the alert from the **Recently Raised Alerts** list.
   - From the **Reports** tab, expand the **Alert Reports** section, then select **All Alerts**, **Critical Alerts**, or **Warning Alerts**. See "Filtering and Controlling the Display of Data in a Report" on page 6-3 to adjust the data in the report.
3. In one of the Alerts pages, select the check boxes for the alerts to which you want to respond.
4. Take 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. Then you must select a distribution list and/or enter email addresses in the **To** or **Cc** fields. Separate multiple email addresses with a comma. Click the **Add to List** button to compile the listing, and then click the **Notify** button to send the notification.
   - **Details.** Select the page icon under the **Details** column for the report, and under the Notes area, enter a note to update the status of the alert.
   - **Set the alert status.** From the **Set Status to** list, select **New** or **Closed**, or a user-defined status value if available, and then click the **Apply** button. When an alert is first generated, it is set to **New**.

A

Oracle Audit Vault and Database Firewall Database Schemas

Topics

About Oracle Audit Vault and Database Firewall Schemas

Oracle Audit Vault and Database Firewall (Oracle AVDF) has internal data warehouse schemas that manage the audit data collected from the secured targets. The data warehouse schemas collect the data from the Oracle AVDF collection agents, organize it, and then provide it in report format for the reports described in Chapter 6, "Generating Reports"

To create custom reports using tools like Oracle Business Intelligence Publisher and the Oracle Business Intelligence Suite:

- You must understand the structure of the data warehouse schema `AVSYS`, which this appendix describes.
- You must understand the structure of the audit events provided by the supported secured targets—Oracle Database, Microsoft SQL Server, Sybase Adaptive Server Enterprise (ASE), and IBM DB2.

  For this information, see Appendix B through Appendix G.

You can create these kinds of custom reports:

- Activity reports
- Event reports
- Alert reports
- Entitlement reports
- Third-party (F5) reports

The data that you need to create the other kinds of reports is in the `AVSYS` schema.

Metadata for Activity Reports

This section describes the metadata that you need to create activity reports:

- Table A–1, " AVSYS.SECURED_TARGET Table"
- Table A–2, " AVSYS.SECURED_TARGET_TYPE Table"
- Table A–3, " AVSYS.AUDIT_TRAIL Table"

Table A–1 describes the AVSYS.SECURED_TARGET table, which has one row for each secured target. Columns are in alphabetical order.

Table A–1 AVSYS.SECURED_TARGET Table

Column	Data Type	Description
ACTIVE	CHAR(1 CHAR)	'Y' if secured target is active, 'N' otherwise.
CONNECT_STRING	VARCHAR2(4000 BYTE)	String that identifies secured target when you try to connect it to the system.
CREATION_TIME	TIMESTAMP WITH LOCAL TIME ZONE	Creation time of the connection between secured target and the system.
DESCRIPTION	VARCHAR2(1024 BYTE)	Description of secured target.
FIREWALL_POLICY_ID	INTEGER	ID number of firewall policy associated with secured target, if any; otherwise NULL. Default: NULL
SECURED_TARGET	NUMBER	Number of secured target.
SECURED_TARGET_NAME	VARCHAR2(255 BYTE)	Name of secured target.
SECURED_TARGET_TYPE_ID	NUMBER	ID number of type of secured target. This value must be in AVSYS.SECURED_TARGET_TYPE.SECURED_TARGET_TYPE_ID (see Table A–2).
SERVER_AUTH_USER	VARCHAR2(255 BYTE)	Oracle AVDF user that is authorized to transfer events from an Audit Vault Agent to an Audit Vault Server.

Table A–2 describes the AVSYS.SECURED_TARGET_TYPE table, which has one row for each secured target type. Columns are in alphabetical order.

Table A–2 AVSYS.SECURED_TARGET_TYPE Table

Column	Data Type	Description
FIREWALL_DIALECT	NUMBER(38)	ID number of Oracle Database Firewall type.
SECURED_TARGET_TYPE_ID	NUMBER(38)	ID number of secured target type.
SECURED_TARGET_TYPE_NAME	VARCHAR2(255 BYTE)	Name of secured target type.

Table A–3 describes the AVSYS.AUDIT_TRAIL table, which has one row for each audit trail. Columns are in alphabetical order.

Table A–3 AVSYS.AUDIT_TRAIL Table

Column	Data Type	Description
AUDIT_TRAIL_ID	NUMBER	ID number of this audit trail.
AUDIT_TRAIL_TYPE	VARCHAR2(255 BYTE)	Type of this audit trail (for example, TABLE or DIRECTORY).
COLLECTION_AUTOSTART	CHAR(1 CHAR)	(Currently unavailable functionality)
HOST_NAME	VARCHAR2(255 BYTE)	Name of agent host for this audit trail.
LOCATION	VARCHAR2(4000 BYTE)	
SOURCE_ID	NUMBER	ID number of source of this audit trail.
SECURED_TARGET_TYPE_NAME	VARCHAR2(255 BYTE)	Name of type of secured target for this audit trail. This value must be in AVSYS.SECURED_TARGET_TYPE.SECURED_TARGET_TYPE_NAME (see Table A–2).

Data for Event Reports

This section describes the data that you need to create event reports.

Table A–4 describes the AVSYS.EVENT_LOG table, which has one row for each audit event. Columns are in alphabetical order.

Table A–4 AVSYS.EVENT_LOG Table

Column	Data Type	Description
ACTION_TAKEN	VARCHAR2(255 BYTE)	Action taken for the event—pass, warn, or block.
ALERT_RAISED	NUMBER	0 if no alert was raised for the event, 1 otherwise. Default: 0
AUDIT_TRAIL_ID	NUMBER	ID of the audit trail from which the event was collected.
AV_TIME	TIMESTAMP WITH LOCAL TIME ZONE	Time when the event was recorded in Oracle AVDF repository.
CLIENT_HOST_NAME	VARCHAR2(255 BYTE)	Name of client host where the user started the action.
CLIENT_IP	VARCHAR2(255 BYTE)	Internet protocol (IP) address of CLIENT_HOST_NAME.
CLIENT_PROGRAM	VARCHAR2(255 CHAR)	Client program where the event occurred.
CLUSTER_ID	NUMBER	Global ID number of cluster where the event occurred.
CLUSTER_TYPE	NUMBER	Type number of cluster where the event occurred (identifies type of statements in cluster).
COMMAND_CLASS	VARCHAR2(255 BYTE)	Action performed in the event (for example, SELECT or DELETE). If this field contains NULL, then the audit record is invalid.
COMMAND_PARAM	CLOB	Command parameters that caused the event.
COMMAND_TEXT	CLOB	Text of command that caused the event (which can be, for example, a SQL or PL/SQL statement).
ERROR_CODE	VARCHAR2(30 BYTE)	Error code of an action.

Table A–4 (Cont.) AVSYS.EVENT_LOG Table

Column	Data Type	Description
ERROR_MESSAGE	VARCHAR2(1000 BYTE)	Error message of an action.
EVENT_NAME	VARCHAR2(255 BYTE)	Name of the event, exactly as in the audit trail.
EVENT_STATUS	VARCHAR2(30 BYTE)	Status of the event—SUCCESS, FAILURE, or UNKNOWN.
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE	Time when the event occurred. If the event has more than one time stamp (for example, an event start time stamp and an event end time stamp), then the collector plug-in must assign a time stamp to this field. If this field contains NULL, then Oracle AVDF shuts down the collector.
EXTENSION	CLOB	Stores fields that cannot be accommodated in core or large fields (such as name-value pairs, separated by delimiters).
GRAMMAR_VERSION	NUMBER	Version of grammar that the Database Firewall used when it detected the event. This version is internal to the Database Firewall and not related to the database version.
LOG_CAUSE	VARCHAR2(30 BYTE)	Cause of the event, as recorded in the log—undefined, exception, cluster, novelty, unseen, invalidsql, waf, login, or logout.
LOGFILE_ID	NUMBER	Opaque internal log file ID.
MARKER	VARCHAR2(255 BYTE)	Uniquely identifies a record in an audit trail. During the recovery process, Oracle AVDF uses this field to filter duplicate records. The collector plug-in provides the marker field, which is typically a concatenated subset of the fields of an audit record. For example, in Oracle database, the session ID and entry ID (a unique identifier within a session) define a marker.
MONITORING_POINT_ID	NUMBER	This is an internal column. If its value is not NULL, then the event came from a Database Firewall. If its value is NULL, then the event came from the audit trail whose ID is in AUDIT_TRAIL_ID.
NETWORK_CONNECTION	VARCHAR2(255 BYTE)	Name of user who logged into the operating system that generated the audit record. If the user logged into the operating system as JOHN but performed the action as SCOTT, then this field contains JOHN and the USER_NAME field contains SCOTT.
OSUSER_NAME	VARCHAR2 (255 BYTE)	Operating system user name that executed the SQL command
POLICY_NAME	VARCHAR2(1024 CHAR)	Name of policy file that the Database Firewall used when it detected the event.
RECORD_ID	NUMBER	ID number of audit record for the event.
SECURED_TARGET_NAME	VARCHAR2(255 BYTE)	Name of secured target where event occurred.

Table A–4 (Cont.) AVSYS.EVENT_LOG Table

Column	Data Type	Description
SECURED_TARGET_TYPE	VARCHAR2(255 BYTE)	Type of secured target where event occurred.
SERVICE_NAME	VARCHAR2(255 CHAR)	Name of database service to which the client session connects.
TARGET_OBJECT	VARCHAR2(255 BYTE)	Name of object on which the action was performed. For example, if the user selected from a table, then this field contains the name of the table.
TARGET_OWNER	VARCHAR2(255 BYTE)	Name of owner of target on which the action was performed. For example, if the user selected from a table owned by user JOHN, then this field contains the user name JOHN.
TARGET_TYPE	VARCHAR2(255 BYTE)	Type of target object on which the action was performed. For example, if the user selected from a table, then this field contains TABLE.
THREAT_SEVERITY	VARCHAR2(30 CHAR)	Severity of the threat that the Database Firewall detected—undefined, insignificant, minor, moderate, major, or catastrophic.
USER_NAME	VARCHAR2(255 BYTE)	Name of user who performed the action in the application or system that generated the audit record. If this field contains NULL, then the audit record is invalid.

Data for Alert Reports

This section describes the data that you need to create alert reports:

- Table A–5, " AVSYS.ALERT_STORE Table"
- Table A–6, " AVSYS.ALERT_EVENT_MAP Table"
- Table A–7, " AVSYS.ALERT_NOTE Table"

Table A–5 describes the AVSYS.ALERT_STORE table, which has one row for each alert instance. Columns are in alphabetical order.

Table A–5 AVSYS.ALERT_STORE Table

Column	Data Type	Description
ALERT_DEFINITION_ID	NUMBER	ID number of definition of this alert.
ALERT_ID	NUMBER	ID number of alert instance.
ALERT_NAME	VARCHAR2(255)	Name of this alert in alert definition.
ALERT_OWNER	VARCHAR2(30)	Alert owner (same as alert definition owner).
ALERT_SEVERITY	NUMBER	Alert severity—1=Warning, 2=Critical.
ALERT_STATUS	VARCHAR2(255)	Alert status—OPEN or CLOSED.
AV_ALERT_TIMESTAMP	TIMESTAMP WITH LOCAL TIME ZONE	Time when alert instance was raised.
CLEARED_TIMESTAMP	TIMESTAMP WITH LOCAL TIME ZONE	
EMAIL_CC_LIST	VARCHAR2(4000 BYTE)	List of addresses for "cc" field of email about this alert instance.

Table A–5 (Cont.) AVSYS.ALERT_STORE Table

Column	Data Type	Description
EMAIL_MESSAGE	VARCHAR2(4000 BYTE)	Message in email about this alert instance.
EMAIL_STATUS	VARCHAR2(30 BYTE)	Indicates if email was sent for this alert instance.
EMAIL_TIMESTAMP	TIMESTAMP WITH LOCAL TIME ZONE	Time when email about this alert instance was sent.
EMAIL_TO_LIST	VARCHAR2(4000 BYTE)	List of addresses for "to" field of email about this alert instance.
ILM_TARGET	VARCHAR2(12)	Information lifecycle management (ILM) string for partition.
OLDEST_EVENT_TIMESTAMP	TIMESTAMP WITH LOCAL TIME ZONE	Time of first event that triggered this alert instance.

Table A–6 describes the AVSYS.ALERT_EVENT_MAP table, which maps each alert instance to its related events. When an alert instance is related to multiple events, each event has a different RECORD_ID. Columns are in alphabetical order.

Table A–6 AVSYS.ALERT_EVENT_MAP Table

Column	Data Type	Description
ALERT_ID	NUMBER	ID of alert instance.
ALERT_OWNER	VARCHAR2(30)	Alert owner, same as alert definition owner.
EVENT_TIMESTAMP	TIMESTAMP WITH LOCAL TIME ZONE	Time of event that triggered this alert instance.
ILM_TARGET	VARCHAR2(12)	ILM string for partition.
OLDEST_EVENT_TIMESTAMP	TIMESTAMP WITH LOCAL TIME ZONE	Time of first event that triggered this alert instance. If this alert instance is related to only one event, then this value is the same as the value of EVENT_TIMESTAMP.
RECORD_ID	NUMBER	Record ID of event related to this alert instance.

Table A–7 describes the AVSYS.ALERT_NOTE table, which stores notes for alert instances. Each alert instance can have multiple notes. Columns are in alphabetical order.

Table A–7 AVSYS.ALERT_NOTE Table

Column	Data Type	Description
ALERT_ID	NUMBER	ID of this note.
ALERT_NOTE_ID	NUMBER	ID of alert instance associated with this note.
HEADER	VARCHAR2(4000 BYTE)	Header of this note.
ILM_TARGET	VARCHAR2(12)	ILM string for partition.
NOTE_CONTENT	VARCHAR2(4000 BYTE)	Content of this note.
NOTE_CREATOR	VARCHAR2(30)	User who created this note.

Table A–7 (Cont.) AVSYS.ALERT_NOTE Table

Column	Data Type	Description
NOTE_OWNER	VARCHAR2(30)	Owner of this note, same as alert definition.
NOTE_TIMESTAMP	TIMESTAMP WITH LOCAL TIME ZONE	Time when this note was created.
OLDEST_EVENT_TIMESTAMP	TIMESTAMP WITH LOCAL TIME ZONE	Time of first event that triggered this alert instance.

Data for Entitlement Reports

This section describes the data that you need to create entitlement reports:

- Table A–8, " AVSYS.UE_DBA_APPLICATION_ROLES"
- Table A–9, " AVSYS.UE_DBA_COL_PRIVS"
- Table A–10, " AVSYS.UE_DBA_PROFILES"
- Table A–11, " AVSYS.UE_DBA_ROLES"
- Table A–12, " AVSYS.UE_DBA_ROLE_PRIVS"
- Table A–13, " AVSYS.UE_DBA_SYS_PRIVS"
- Table A–14, " AVSYS.UE_DBA_TAB_PRIVS"
- Table A–15, " AVSYS.UE_DBA_USERS"
- Table A–16, " AVSYS.UE_ROLE_SYS_PRIVS"
- Table A–17, " AVSYS.UE_ROLE_TAB_PRIVS"
- Table A–18, " AVSYS.UE_SYS_DBA_OPER_USERS"

Note: In each of the preceding table names, "UE" means "User Entitlement."

Table A–8 describes the AVSYS.UE_DBA_APPLICATION_ROLES table, which stores information about roles granted to Oracle Database packages. Columns are in alphabetical order.

Table A–8 AVSYS.UE_DBA_APPLICATION_ROLES

Column	Data Type	Description
PACKAGE	VARCHAR2 (30)	Name of Oracle Database package to which role was granted
ROLE	VARCHAR2 (30)	Role granted to package
SCHEMA	VARCHAR2 (30)	Schema to which package belongs
SNAPSHOT_ID	NUMBER	Snapshot ID

Table A–9 describes the AVSYS.UE_DBA_COL_PRIVS table, which stores information about privileges granted to users on individual columns of Oracle Database tables. Columns are in alphabetical order.

Table A–9 AVSYS.UE_DBA_COL_PRIVS

Column	Data Type	Description
COMMON	VARCHAR2 (3)	For Oracle Database 12*c*, whether the user is common to a CDB and PDB: ■ Y - user is common to both ■ N - user is local to PDB ■ Null - database is not a CDB or PDB
CONTAINER	VARCHAR2 (30)	For Oracle Database 12*c*, the container (CDB) identifier.
COLUMN_NAME	VARCHAR2 (30)	Name of column on which privilege was granted
GRANTABLE	VARCHAR2 (3)	Whether the privilege was granted with the GRANTABLE option—YES or NO
GRANTEE	VARCHAR2 (30)	User to whom the column privilege was granted
GRANTOR	VARCHAR2 (30)	User who granted the column privilege to GRANTEE
OWNER	VARCHAR2 (30)	Column privilege owner
PRIVILEGE	VARCHAR2 (40)	Column privilege
SNAPSHOT_ID	NUMBER	Snapshot ID
TABLE_NAME	VARCHAR2 (30)	Name of Oracle Database table to which column belongs

Table A–10 describes the AVSYS.UE_DBA_PROFILES table, which stores information about Oracle Database profiles. Columns are in alphabetical order.

Table A–10 AVSYS.UE_DBA_PROFILES

Column	Data Type	Description
COMMON	VARCHAR2 (3)	For Oracle Database 12*c*, whether the user is common to a CDB and PDB: ■ Y - user is common to both ■ N - user is local to PDB ■ Null - database is not a CDB or PDB
CONTAINER	VARCHAR2 (30)	For Oracle Database 12*c*, the container (CDB) identifier.
LIMIT	VARCHAR2 (40)	Profile limit
PROFILE	VARCHAR2 (30)	Profile name
RESOURCE_NAME	VARCHAR2 (32)	Resource name
RESOURCE_TYPE	VARCHAR2 (8)	Resource type
SNAPSHOT_ID	NUMBER	Snapshot ID

Table A–11 describes the AVSYS.UE_DBA_ROLES table, which stores information about Oracle Database roles. The table has one row for each role. Columns are in alphabetical order.

Table A–11 AVSYS.UE_DBA_ROLES

Column	Data Type	Description
AUTHENTICATION_TYPE	VARCHAR2 (8)	Authentication mechanism for this user: ■ EXTERNAL - CREATE USER user1 IDENTIFIED EXTERNALLY ■ GLOBAL - CREATE USER user2 IDENTIFIED GLOBALLY ■ PASSWORD - CREATE USER user3 IDENTIFIED BY user3
COMMON	VARCHAR2 (3)	For Oracle Database 12*c*, whether the user is common to a CDB and PDB: ■ Y - user is common to both ■ N - user is local to PDB ■ Null - database is not a CDB or PDB
CONTAINER	VARCHAR2 (30)	For Oracle Database 12*c*, the container (CDB) identifier.
PASSWORD_REQUIRED	VARCHAR2 (8)	Whether the role requires a password—YES or NO
ROLE	VARCHAR2 (30)	Name of the role
SNAPSHOT_ID	NUMBER	Snapshot ID

Table A–12 describes the AVSYS.UE_DBA_ROLE_PRIVS table, which stores information about the roles granted to users and roles. Columns are in alphabetical order.

Table A–12 AVSYS.UE_DBA_ROLE_PRIVS

Column	Data Type	Description
COMMON	VARCHAR2 (3)	For Oracle Database 12*c*, whether the user is common to a CDB and PDB: ■ Y - user is common to both ■ N - user is local to PDB ■ Null - database is not a CDB or PDB
CONTAINER	VARCHAR2 (30)	For Oracle Database 12*c*, the container (CDB) identifier.
ADMIN_OPTION	VARCHAR2 (3)	Whether the privilege was granted with the ADMIN option—YES or NO
DEFAULT_ROLE	VARCHAR2 (3)	Whether the role is the default role for the user—YES or NO
GRANTED_ROLE	VARCHAR2 (30)	Name of the role granted to the user or role
GRANTEE	VARCHAR2 (30)	Name of the user or role to which the GRANTED_ROLE was granted
SNAPSHOT_ID	NUMBER	Snapshot ID

Table A–13 describes the AVSYS.UE_DBA_SYS_PRIVS table, which stores information about the system privileges granted to users and roles. Columns are in alphabetical order.

Table A–13 AVSYS.UE_DBA_SYS_PRIVS

Column	Data Type	Description
COMMON	VARCHAR2 (3)	For Oracle Database 12*c*, whether the user is common to a CDB and PDB: ■ Y - user is common to both ■ N - user is local to PDB ■ Null - database is not a CDB or PDB
CONTAINER	VARCHAR2 (30)	For Oracle Database 12*c*, the container (CDB) identifier.
ADMIN_OPTION	VARCHAR2 (3)	Whether the privilege was granted with the ADMIN option—YES or NO
GRANTEE	VARCHAR2 (30)	Name of the user or role to whom the system privilege was granted
PRIVILEGE	VARCHAR2 (40)	System privilege
SNAPSHOT_ID	NUMBER	Snapshot ID

Table A–14 describes the AVSYS.UE_DBA_TAB_PRIVS table, which stores information about the privileges granted to users on objects. Columns are in alphabetical order.

Table A–14 AVSYS.UE_DBA_TAB_PRIVS

Column	Data Type	Description
COMMON	VARCHAR2 (3)	For Oracle Database 12*c*, whether the user is common to a CDB and PDB: ■ Y - user is common to both ■ N - user is local to PDB ■ Null - database is not a CDB or PDB
CONTAINER	VARCHAR2 (30)	For Oracle Database 12*c*, the container (CDB) identifier.
GRANTABLE	VARCHAR2 (3)	Whether the privilege was granted with the GRANTABLE option—YES or NO
GRANTEE	VARCHAR2 (30)	User to whom the privilege was granted
GRANTOR	VARCHAR2 (30)	User who granted the privilege to GRANTEE
HIERARCHY	VARCHAR2 (3)	Whether the privilege was granted with the HIERARCHY option—YES or NO
OWNER	VARCHAR2 (30)	Owner of the object
PRIVILEGE	VARCHAR2 (40)	Privilege on the object
SNAPSHOT_ID	NUMBER	Snapshot ID
TABLE_NAME	VARCHAR2 (30)	Name of the object on which privilege was granted
TYPE	VARCHAR2 (24)	Object type (table, view, sequence, etc.)

Table A–15 describes the AVSYS.UE_DBA_USERS table, which has a row for every Oracle Database user. Columns are in alphabetical order.

Table A–15 AVSYS.UE_DBA_USERS

Column	Data Type	Description
ACCOUNT_STATUS	VARCHAR2 (32)	User account status, which is one of these: ■ OPEN ■ EXPIRED ■ EXPIRED(GRACE) ■ LOCKED(TIMED) ■ LOCKED ■ EXPIRED & LOCKED(TIMED) ■ EXPIRED(GRACE) & LOCKED(TIMED) ■ EXPIRED & LOCKED ■ EXPIRED(GRACE) & LOCKED
AUTHENTICATION_TYPE	VARCHAR2 (8)	Authentication mechanism for this user: ■ EXTERNAL - CREATE USER user1 IDENTIFIED EXTERNALLY ■ GLOBAL - CREATE USER user2 IDENTIFIED GLOBALLY ■ PASSWORD - CREATE USER user3 IDENTIFIED BY user3
COMMON	VARCHAR2 (3)	For Oracle Database 12*c*, whether the user is common to a CDB and PDB: ■ Y - user is common to both ■ N - user is local to PDB ■ Null - database is not a CDB or PDB
CONTAINER	VARCHAR2 (30)	For Oracle Database 12*c*, the container (CDB) identifier.
CREATED	TIMESTAMP (0) WITH LOCAL TIME ZONE	Date when user account was created
DEFAULT_TABLESPACE	VARCHAR2 (30)	Default tablespace for user
EDITIONS_ENABLED	VARCHAR2 (1)	Indicates whether editions have been enabled for the corresponding user (Y or N)
EXPIRY_DATE	TIMESTAMP (0) WITH LOCAL TIME ZONE	Date when user account expires or expired
EXTERNAL_NAME	VARCHAR2 (4000)	External name of user
INITIAL_RSRC_CONSUMER_GROUP	VARCHAR2 (30)	Initial resource consumer group
LAST_LOGON	TIMESTAMP (9) WITH LOCAL TIME ZONE	For Oracle Database 12*c*, time when user last logged on
LOCK_DATE	TIMESTAMP (0) WITH LOCAL TIME ZONE	Date when user account was locked
ORACLE_MAINTAINED	CHAR (1)	For Oracle Database 12*c*, whether user was created, and is maintained, by Oracle-supplied scripts. A value of Y means that user must not be changed in any way except by running an Oracle-supplied script.
PROFILE	VARCHAR2 (30)	User profile

Table A–15 (Cont.) AVSYS.UE_DBA_USERS

Column	Data Type	Description
PROXY_ONLY_CONNECT	CHAR (1)	For Oracle Database 12*c*, whether this user can connect only through a proxy
SNAPSHOT_ID	NUMBER	Snapshot ID
TEMPORARY_TABLESPACE	VARCHAR2 (30)	Temporary tablespace for user
USERNAME	VARCHAR2 (30)	Oracle Database user name

Table A–16 describes the AVSYS.UE_ROLE_SYS_PRIVS table, which stores information about system privileges granted to roles. Columns are in alphabetical order.

Table A–16 AVSYS.UE_ROLE_SYS_PRIVS

Column	Data Type	Description
COMMON	VARCHAR2 (3)	For Oracle Database 12*c*, whether the user is common to a CDB and PDB: ■ Y - user is common to both ■ N - user is local to PDB ■ Null - database is not a CDB or PDB
ADMIN_OPTION	VARCHAR2 (3)	Whether the privilege was granted with the ADMIN option—YES or NO
PRIVILEGE	VARCHAR2 (40)	System privilege granted to the role
ROLE	VARCHAR2 (30)	Name of role
SNAPSHOT_ID	NUMBER	Snapshot ID

Table A–17 describes the AVSYS.UE_ROLE_TAB_PRIVS table, which stores information about the table privileges granted to roles. Columns are in alphabetical order.

Table A–17 AVSYS.UE_ROLE_TAB_PRIVS

Column	Data Type	Description
COLUMN_NAME	VARCHAR2 (30)	Name of column on which privilege was granted
COMMON	VARCHAR2 (3)	For Oracle Database 12*c*, whether the user is common to a CDB and PDB: ■ Y - user is common to both ■ N - user is local to PDB ■ Null - database is not a CDB or PDB
GRANTABLE	VARCHAR2 (3)	Whether the privilege was granted with the GRANTABLE option—YES or NO
OWNER	VARCHAR2 (30)	Table privilege owner
PRIVILEGE	VARCHAR2 (40)	Table privilege
ROLE	VARCHAR2 (30)	Role to which table privilege was granted
TABLE_NAME	VARCHAR2 (30)	Name of Oracle Database table on which privilege was granted
UE_SNAPSHOT_SNAPSHOT_ID	NUMBER	Snapshot ID

Table A–18 describes the AVSYS.UE_SYS_DBA_OPER_USERS table, which stores information about all users in the password file. Columns are in alphabetical order.

Table A–18 AVSYS.UE_SYS_DBA_OPER_USERS

Column	Data Type	Description
CONTAINER	VARCHAR2 (30)	For Oracle Database 12*c*, the container (CDB) identifier.
SNAPSHOT_ID	NUMBER	Snapshot ID
SYSASM	VARCHAR2 (5)	Whether the user can connect to the database with the SYSASM privilege—TRUE or FALSE.
SYSBACKUP	VARCHAR2 (5)	Whether the user can connect to the database with the SYSBACKUP privilege—TRUE or FALSE.
SYSDBA	VARCHAR2 (5)	Whether the user can connect to the database with the SYSDBA privilege—TRUE or FALSE.
SYSDG	VARCHAR2 (5)	Whether the user can connect to the database with the SYSDG privilege—TRUE or FALSE.
SYSKM	VARCHAR2 (5)	Whether the user can connect to the database with the SYSKM privilege—TRUE or FALSE.
SYSOPER	VARCHAR2 (8)	Whether the user can connect to the database with the SYSOPER privilege—TRUE or FALSE.
USERNAME	VARCHAR2 (30)	User name in the password file

Data for SPA Reports

This section describes data that you need to create custom Stored Procedure Auditing (SPA) reports:

- Table A–19, " AVSYS.SPA_OBJECTS"
- Table A–20, " AVSYS.SPA_EDITS"

Table A–19 describes the AVSYS.SPA_OBJECTS table, which stores summary data about stored procedure objects.

Table A–19 AVSYS.SPA_OBJECTS

Column	Data Type	Description
ID	INTEGER	Unique identifier for the object
SECURED_TARGET_ID	INTEGER	The secured target source of database objects
OBJECT_SUBTYPE	VARCHAR2(40 BYTE)	The subtype of the object
OBJECT_CLASS	VARCHAR2(40 BYTE)	The class of the object
NAME	VARCHAR2 (1024 CHAR)	The name of the object
CHANGED_BY	VARCHAR2 (2048 CHAR)	Coma separated database users that modified the object
LAST_CHANGED_AT	TIMESTAMP WITH LOCAL TIME ZONE	The date and time when the object was changed
LAST_SIGNATURE	VARCHAR2 (40 BYTE)	The hash of the object (signature change means object change)
LAST_EDIT_TYPE	VARCHAR2 (40 BYTE)	The most recent type of the change
EDIT_CNT_NEW	INTEGER	Keeps the number of "new" edit records is for this object
EDIT_CNT_MODIFY	INTEGER	Keeps the number of "modify" edit records is for this object

Table A–19 (Cont.) AVSYS.SPA_OBJECTS

Column	Data Type	Description
EDIT_CNT_DELETE	INTEGER	Keeps the number of "delete" edit records is for this object
CHANGES_SUMMARY	VARCHAR2(255 CHAR)	The summary of the changes
UPDATED_AT	TIMESTAMP WITH LOCAL TIME ZONE	The date and time when the record was updated by the Database Firewall software

Table A–20 describes the AVSYS.SPA_EDITS table, which stores data about, and the content of, stored procedure edits.

Table A–20 AVSYS.SPA_EDITS

Column	Data Type	Description
ID	INTEGER	Unique identifier for the object
OBJECT_ID	INTEGER	Foreign key that references the ID column of the AVSYS.SPA_OBJECTS table
SIGNATURE	VARCHAR2 (40 BYTE)	The hash of the object (signature change means object change)
CONTENT	CLOB	The new content of the object
EDIT_TYPE	VARCHAR2 (40 BYTE)	The type of the change
CHANGED_BY	VARCHAR2 (2048 CHAR)	The database user that modified the object
CHANGED_AT	TIMESTAMP WITH LOCAL TIME ZONE	The date and time when the object was changed
DETECTED_AT	TIMESTAMP WITH LOCAL TIME ZONE	The date and time when the change was detected on the controller

Data for Database Firewall Reports

This section describes data that you need to create custom Database Firewall reports:

- Table A–21, " AVSYS.FW_CLUSTER"
- Table A–22, " AVSYS.FW_CLUSTER_COMPONENT"

Table A–21 describes the AVSYS.FW_CLUSTERS table, which provides summary data on cluster traffic to secured target databases, and gives an example statement that would appear in a given cluster.

Table A–21 AVSYS.FW_CLUSTER

Column	Data Type	Description
ID	NUMBER	Cluster global identifier
SECURED_TARGET_ID	INTEGER	The secured target database for this cluster
CLUSTER_HASH	INTEGER	The hash of the cluster
GRAMMAR_VERSION	INTEGER	Version number of the Database Firewall grammar
FIREWALL_DIALECT	SMALLINTEGER	Database type of the cluster (see AVSYS.SECURED_TARGET_TYPE Table on page A-2 for meaning)
CLUSTER_TYPE	VARCHAR2 (40 BYTE)	Type of statements included in the cluster
REPRESENTATION	CLOB	Cluster path representation
CLUSTER_EXAMPLE	CLOB	An example statement in the cluster

Table A–22 describes the AVSYS.FW_CLUSTER_COMPONENTS table, which provides cluster data broken down into cluster components. This data may be used, for example, to report on clusters related to a specific database table or table column.

Table A–22 AVSYS.FW_CLUSTER_COMPONENT

Column	Data Type	Description
CLUSTER_ID	INTEGER	Foreign key that references the ID column of the AVSYS.FW_CLUSTERS table
COMPONENT_INDEX	INTEGER	Index of the component (starts with 1)
COMPONENT_TYPE	VARCHAR2(50 BYTE)	Component type may be one of: 'keyword', 'column', 'table', 'procedure', 'cluster_set', 'function', '_'
COMPONENT_VALUE	VARCHAR2(4000 CHAR)	The component string
COMPONENT_USAGE	VARCHAR2(50 BYTE)	Component usage may be one of: NULL, 'read', 'write', 'define', 'call', 'control'

B

Audit Record Fields

Table B–1 lists the fields in an Oracle AVDF audit record.

Table B–1 Audit Record Fields

Audit Record Field	Description	Column Type
Secured Target Name	Target system secured by AVDF	varchar2(255)
Secured Target Type	Type of secured target, for example, Microsoft SQL Server, IBM DB2 etc.	varchar2(255)
Service Name	Secured target service used to perform this event	varchar2 (255 char)
Policy Name	Name of the policy when the event was recorded	varchar2(1024)
Event Server Time	Time of entry of the audit record in the Audit Vault Server	Timestamp with local timezone
Event Time	Time of event occurrence	timestamp with local timezone
User Name	Secured target user that performed the event	varchar2(255)
Event Status	Status of completion of the event	varchar2(30)
Error Code	Error number on event failure	varchar2(30)
Error Message	Error message on event failure	varchar2(1000)
Event Name	Name of the event as recognized by the secured target	varchar2(255)
Action Taken	Action taken on the command	varchar2(255)
Threat Severity	Threat severity assigned to the command	varchar2(30 char)
Log Cause	Reason for logging the event	NUMBER - Max 22 bytes
Target Object	Object affected by event	varchar2(255)
Target Type	Type of target object, for example, Package, Type, Table	varchar2(255)
Target Owner	Owner of target object	varchar2(255)
OS User Name	Operating system login name of the secured target user causing the event	varchar2(255)
Client Host Name	Name of the host machine	varchar2(255)
Client IP	IP address of the Client Host	varchar2(255)
Network Connection	Description of the network connection	varchar2(255)

Table B–1 (Cont.) Audit Record Fields

Audit Record Field	Description	Column Type
Client Program	Name of program on Client Host that issued command	varchar2(255)
Command Text	Command statement issued by secured target user	CLOB Securefile
Command Param	Parameters associated with command text	CLO
Extension	Additional detailed information about the audited event	CLOB Securefile
Original Content	Audit record generated by secured target	CLOB Securefile
Command Class	Class of command issued by secured target user that caused the event	varchar2(255)

C

Oracle Database Audit Events

Topics

About the Oracle Database Audit Events

This appendix maps audit event names used in the Oracle Database to their equivalent values in the **command_class** and **target_type** fields in the Oracle AVDF audit record. The audit events are organized in useful categories, for example, Account Management events. You can use the audit events mapped here to create custom audit reports using other Oracle Database reporting products or third-party tools. See also "Oracle Audit Vault and Database Firewall Database Schemas" on page A-1 for Oracle AVDF data warehouse details that may be useful in designing your own reports.

Account Management Events

Account management events track SQL statements that affect user accounts, such as creating users or altering their profiles.

Table C–1 lists the Oracle Database account management audit events and the equivalent Oracle AVDF events.

Table C–1 Oracle Database Account Management Audit Events

Source Event	Event Description	command_class	target_type
ALTER PROFILE	Alter Profile	ALTER	PROFILE
ALTER USER	Alter User	ALTER	USER
CREATE PROFILE	Create Profile	CREATE	PROFILE
CREATE USER	Create User	CREATE	USER
DROP PROFILE	Drop Profile	DROP	PROFILE
DROP USER	Drop User	DROP	USER

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.

Table C–2 lists the Oracle Database application management audit events and the equivalent Oracle AVDF events.

Table C–2 Oracle Database Application Management Audit Events

Source Event	Event Description	command_class	target_type
ALTER ASSEMBLY	Alter Assembly (Release 11.2)	ALTER	ASSEMBLY
ALTER FUNCTION	Alter Function	ALTER	FUNCTION
ALTER JAVA	Alter Java	ALTER	JAVA
ALTER PACKAGE	Alter Package	ALTER	PACKAGE
ALTER PACKAGE BODY	Alter Package Body	ALTER	PACKAGE BODY
ALTER PROCEDURE	Alter Procedure	ALTER	PROCEDURE
ALTER RESOURCE COST	Alter Resource Cost	ALTER	RESOURCE COST
ALTER REWRITE EQUIVALENCE	Alter Rewrite Equivalence	ALTER	REWRITE EQUIVALENCE
ALTER TRIGGER	Alter Trigger	ALTER	TRIGGER
ALTER TYPE	Alter Type	ALTER	TYPE
ALTER TYPE BODY	Alter Type Body	ALTER	TYPE BODY
ANALYZE INDEX	Analyze Index	ANALYZE	INDEX
ANALYZE TABLE	Analyze Table	ANALYZE	TABLE
ASSOCIATE STATISTICS	Associate Statistics	ASSOCIATE	STATISTICS
CREATE ASSEMBLY	Create Assembly (Release 11.2)	CREATE	ASSEMBLY
CREATE CONTEXT	Create Context	CREATE	CONTEXT
CREATE FUNCTION	Create Function	CREATE	FUNCTION
CREATE INDEXTYPE	Create IndexType	CREATE	INDEXTYPE
CREATE JAVA	Create Java	CREATE	JAVA

Table C–2 (Cont.) Oracle Database Application Management Audit Events

Source Event	Event Description	command_class	target_type
CREATE LIBRARY	Create Library	CREATE	LIBRARY
CREATE OPERATOR	Create Operator	CREATE	OPERATOR
CREATE PACKAGE	Create Package	CREATE	PACKAGE
CREATE PACKAGE BODY	Create Package Body	CREATE	PACKAGE BODY
CREATE PROCEDURE	Create Procedure	CREATE	PROCEDURE
CREATE TRIGGER	Create Trigger	CREATE	TRIGGER
CREATE TYPE	Create Type	CREATE	TYPE
CREATE TYPE BODY	Create Type Body	CREATE	TYPE BODY
DECLARE REWRITE EQUIVALENCE	Declare Rewrite Equivalence	SET	REWRITE EQUIVALENCE
DISABLE TRIGGER	Disable Trigger	DISABLE	TRIGGER
DISASSOCIATE STATISTICS	Disassociate Statistics	DISASSOCIATE	STATISTICS
DROP ASSEMBLY	Drop Assembly (Release 11.2)	DROP	ASSEMBLY
DROP CONTEXT	Drop Context	DROP	CONTEXT
DROP FUNCTION	Drop Function	DROP	FUNCTION
DROP INDEXTYPE	Drop Indextype	DROP	INDEXTYPE
DROP JAVA	Drop Java	DROP	JAVA
DROP LIBRARY	Drop Library	DROP	LIBRARY
DROP OPERATOR	Drop Operator	DROP	OPERATOR
DROP PACKAGE	Drop Package	DROP	PACKAGE
DROP PACKAGE BODY	Drop Package Body	DROP	PACKAGE BODY
DROP PROCEDURE	Drop Procedure	DROP	PROCEDURE
DROP REWRITE EQUIVALENCE	Drop Rewrite Equivalence	DROP	REWRITE EQUIVALENCE
DROP TRIGGER	Drop Trigger	DROP	TRIGGER
DROP TYPE	Drop Type	DROP	TYPE
DROP TYPE BODY	Drop Type Body	DROP	TYPE BODY
ENABLE TRIGGER	Enable Trigger	ENABLE	TRIGGER
EXECUTE TYPE	Execute Type	EXECUTE	TYPE
EXPLAIN	Explain	EXPLAIN	NULL

Audit Command Events

Audit command events track the use of AUDIT SQL statements on other SQL statements and on database objects.

Table C–3 lists the Oracle Database audit command audit events and the equivalent Oracle AVDF events.

Table C–3 Oracle Database Audit Command Audit Events

Source Event	Event Description	command_class	target_type
AUDIT DEFAULT	Audit Default	AUDIT	DEFAULT
AUDIT OBJECT	Audit Object	AUDIT	OBJECT
NOAUDIT DEFAULT	NoAudit default	NOAUDIT	DEFAULT
NOAUDIT OBJECT	NoAudit Subject	NOAUDIT	OBJECT
AUDIT SYSTEM	System Audit	AUDIT	SYSTEM
NOAUDIT SYSTEM	System No Audit	NOAUDIT	SYSTEM

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 "Data Access Report" on page 6-17, uses these events.

Table C–4 lists the Oracle Database data access audit events and the equivalent Oracle AVDF events.

Table C–4 Oracle Database Data Access Audit Events

Source Event	Event Description	command_ class	target_type
DELETE	Delete	DELETE	NULL
INSERT	Insert	INSERT	NULL
SELECT	Select	SELECT	NULL
MINING MODEL	Select Mining Model (Release 11.2)	SELECT	MINING MODEL
TRUNCATE TABLE	Truncate Table	TRUNCATE	TRUNCATE TABLE
UPDATE	Update	UPDATE	NULL

Database Vault Events

Topics

Database Vault Events in Oracle Database 11g

Table C–5 lists Database Vault events for Oracle Database 11*g* databases that have Database Vault enabled.

Table C–5 Database Vault Audit Events in Oracle Database 11g

Source Event	Event Description	command_ class	target_type
FACTOR EVALUATION	Factor Evaluation	EXECUTE	FACTOR
FACTOR ASSIGNMENT	Factor Assignment	ASSIGN	FACTOR
FACTOR EXPRESSION	Factor Expression	EXECUTE	FACTOR
REALM VIOLATION	Realm Violation	VIOLATE	REALM
REALM AUTHORIZATION	Realm Authorization	AUTHORIZE	REALM
COMMAND AUTHORIZATION	Command Authorization	AUTHORIZE	COMMAND
SECURE ROLE	Secure Role	SECURE	ROLE
ACCESS CTRL SESSION INIT	Access Control Session Initialization	INITIALIZE	ACCESS CONTROL SESSION
ACCESS CTRL COMMAND AUTH	Access Control Command Authorization	AUTHORIZE	ACCESS CONTROL COMMAND
LBL SEC SESSION INIT	Label Security Session Initialization	INITIALIZE	LABEL SECURITY SESSION
LBL SEC ATTEMPT TO UPGRADE	Label Security Attempt to Upgrade	UPDATE	LABEL SECURITY

Database Vault Events in Oracle Database 12c

Table C–6 lists Database Vault events for Oracle Database 12*c* databases that have Database Vault enabled.

Table C–6 Database Vault Audit Events in Oracle Database 12c

Source Event	Event Description	command_ class	target_type
FACTOR EVALUATION AUDIT	Factor Evaluation Audit	EXECUTE	FACTOR
FACTOR ASSIGNMENT AUDIT	Factor Assignment Audit	ASSIGN	FACTOR
FACTOR EXPRESSION AUDIT	Factor Expression Audit	EXECUTE	FACTOR
REALM VIOLATION AUDIT	Realm Violation Audit	VIOLATE	REALM
REALM AUTHORIZATION AUDIT	Realm Authorization Audit	AUTHORIZE	REALM
COMMAND AUTHORIZATION AUDIT	Command Authorization Audit	AUTHORIZE	COMMAND
SECURE ROLE AUDIT	Secure Role Audit	SECURE	ROLE
SESSION INITIALIZATION AUDIT	Session Initialization Audit	INITIALIZE	SESSION
OLS SESSION INITIALIZATION AUDIT	OLS Session Initialization Audit	INITIALIZE	LABEL SESSION

Table C–6 (Cont.) Database Vault Audit Events in Oracle Database 12c

Source Event	Event Description	command_ class	target_type
OLS ATTEMPT TO UPGRADE LABEL AUDIT	OLS Attempt To Upgrade Label Audit	UPDATE	LABEL SECURITY
ENABLE DV ENFORCEMENT AUDIT	Enable DV Enforcement Audit	ENABLE	DV ENFORCEMENT
DISABLE DV ENFORCEMENT AUDIT	Disable DV Enforcement Audit	DISABLE	DV ENFORCEMENT
REALM CREATION AUDIT	Realm Creation Audit	CREATE	REALM
REALM UPDATE AUDIT	REALM UPDATE AUDIT	UPDATE	REALM
REALM RENAME AUDIT	Realm Rename Audit	RENAME	REALM
REALM DELETION AUDIT	Realm Deletion Audit	DELETE	REALM
ADD REALM AUTH AUDIT	Add Realm Auth Audit	ADD	REALM AUTH
DELETE REALM AUTH AUDIT	Delete Realm Auth Audit	DELETE	REALM AUTH
UPDATE REALM AUTH AUDIT	Update Realm Auth Audit	UPDATE	REALM AUTH
ADD REALM OBJECT AUDIT	Add Realm Object Audit	ADD	REALM OBJECT
UPDATE REALM OBJECT AUDIT	Update Realm Object Audit	UPDATE	REALM OBJECT
DELETE REALM OBJECT AUDIT	Delete Realm Object Audit	DELETE	REALM OBJECT
ENABLE EVENT AUDIT	Enable Event Audit	ENABLE	EVENT
DISABLE EVENT AUDIT	Disable Event Audit	DISABLE	EVENT
RULE SET CREATION AUDIT	Rule Set Creation Audit	CREATE	RULE SET
RULE SET UPDATE AUDIT	Rule Set Update Audit	UPDATE	RULE SET
RULE SET RENAME AUDIT	Rule Set Rename Audit	RENAME	RULE SET
RULE SET DELETION AUDIT	Rule Set Deletion Audit	DELETE	RULE SET
ADD RULE TO RULE SET AUDIT	Add Rule to Rule Set Audit	ADD	RULE SET
DELETE RULE FROM RULE SET AUDIT	Delete Rule from Rule Set Audit	DELETE	RULE SET
RULE CREATION AUDIT	Rule Creation Audit	CREATE	RULE
RULE UPDATE AUDIT	Rule Update Audit	UPDATE	RULE
RULE RENAME AUDIT	Rule Rename Audit	RENAME	RULE
RULE DELETION AUDIT	Rule Deletion Audit	DELETE	RULE
COMMANDRULE CREATION AUDIT	Command Rule Creation Audit	CREATE	COMMANDRULE
COMMANDRULE UPDATE AUDIT	Command Rule Update Audit	UPDATE	COMMANDRULE
COMMANDRULE DELETION AUDIT	Command Rule Deletion Audit	DELETE	COMMANDRULE

Table C–6 (Cont.) Database Vault Audit Events in Oracle Database 12c

Source Event	Event Description	command_ class	target_type
AUTHORIZE DATAPUMP USER AUDIT	Authorize Datapump User Audit	AUTHORIZE	DATAPUMP USER
UNAUTHORIZE DATAPUMP USER AUDIT	Unauthorize Datapump User Audit	REVOKE	DATAPUMP USER
AUTHORIZE JOB USER AUDIT	Authorize Job User Audit	AUTHORIZE	JOB USER
UNAUTHORIZE JOB USER AUDIT	Unauthorize Job User Audit	REVOKE	JOB USER
FACTOR_TYPE CREATION AUDIT	Factor Type Creation Audit	CREATE	FACTOR TYPE
FACTOR_TYPE DELETION AUDIT	Factor Type Deletion Audit	DELETE	FACTOR TYPE
FACTOR_TYPE UPDATE AUDIT	Factor Type Update Audit	UPDATE	FACTOR TYPE
FACTOR_TYPE RENAME AUDIT	Factor Type Rename Audit	RENAME	FACTOR TYPE
FACTOR CREATION AUDIT	Factor Creation Audit	CREATE	FACTOR
FACTOR DELETION AUDIT	Factor Deletion Audit	DELETE	FACTOR
FACTOR UPDATE AUDIT	Factor Update Audit	UPDATE	FACTOR
FACTOR RENAME AUDIT	Factor Rename Audit	RENAME	FACTOR
ADD FACTOR LINK AUDIT	Add Factor Link Audit	ADD	FACTOR LINK
DELETE FACTOR LINK AUDIT	Delete Factor Link Audit	DELETE	FACTOR LINK
ADD POLICY FACTOR AUDIT	Add Policy Factor Audit	ADD	POLICY FACTOR
DELETE POLICY FACTOR AUDIT	Delete Policy Factor Audit	DELETE	POLICY FACTOR
CREATE IDENTITY AUDIT	Create Identity Audit	CREATE	IDENTITY
DELETE IDENTITY AUDIT	Delete Identity Audit	DELETE	IDENTITY
UPDATE IDENTITY AUDIT	Update Identity Audit	UPDATE	IDENTITY
CHANGE IDENTITY FACTOR AUDIT	Change Identity Factor Audit	UPDATE	IDENTITY FACTOR
CHANGE IDENTITY VALUE AUDIT	Change Identity Value Audit	UPDATE	IDENTITY VALUE
CREATE IDENTITY MAP AUDIT	Create Identity Map Audit	CREATE	IDENTITY MAP
DELETE IDENTITY MAP AUDIT	Delete Identity Map Audit	DELETE	IDENTITY MAP
CREATE POLICY LABEL AUDIT	Create Policy Label Audit	CREATE	LABEL POLICY
DELETE POLICY LABEL AUDIT	Delete Policy Label Audit	DELETE	LABEL POLICY
CREATE MAC POLICY AUDIT	Create Mac Policy Audit	CREATE	MAC POLICY

Table C–6 (Cont.) Database Vault Audit Events in Oracle Database 12c

Source Event	Event Description	command_ class	target_type
UPDATE MAC POLICY AUDIT	Update MAC Policy Audit	UPDATE	MAC POLICY
DELETE MAC POLICY AUDIT	Delete MAC Policy Audit	DELETE	MAC POLICY
CREATE ROLE AUDIT	Create Role Audit	CREATE	ROLE
DELETE ROLE AUDIT	Delete Role Audit	DELETE	ROLE
UPDATE ROLE AUDIT	Update Role Audit	UPDATE	ROLE
RENAME ROLE AUDIT	Rename Role Audit	RENAME	ROLE
CREATE DOMAIN IDENTITY AUDIT	Create Domain Identity Audit	CREATE	DOMAIN IDENTITY
DROP DOMAIN IDENTITY AUDIT	Drop Domain Identity Audit	DROP	DOMAIN IDENTITY
ENABLE ORADEBUG AUDIT	Enable ORADEBUG Audit	ENABLE	ORADEBUG
DISABLE ORADEBUG AUDIT	Disable ORADEBUG Audit	DISABLE	ORADEBUG
COMMAND FAILURE AUDIT	Command Failure Audit	FAIL	COMMAND
AUTHORIZE PROXY USER AUDIT	Authorize Proxy User Audit	AUTHORIZE	PROXY USER
UNAUTHORIZE PROXY USER AUDIT	Unauthorize Proxy User Audit	REVOKE	PROXY USER
ENABLE DV DICTIONARY ACCOUNTS AUDIT	Enable DV Dictionary Accounts Audit	ENABLE	DV DICTIONARY ACCOUNT
DISABLE DV DICTIONARY ACCOUNTS AUDIT	Disable DV Dictionary Accounts Audit	DISABLE	DV DICTIONARY ACCOUNT
AUTHORIZE DDL AUDIT	Authorize DDL Audit	AUTHORIZE	DDL
UNAUTHORIZE DDL AUDIT	Unauthorize DDL Audit	REVOKE	DDL
AUTHORIZE TTS AUDIT	Authorize Transportable Tablespace Audit	AUTHORIZE	TRANSPORTABLE TABLESPACE
UNAUTHORIZE TTS AUDIT	Unauthorize Transportable Tablespace Audit	REVOKE	TRANSPORTABLE TABLESPACE

Exception Events

Exception events track audited error and exception activity, such as network errors. Table C–7 lists the Oracle Database exception audit events and the equivalent Oracle AVDF event.

Table C–7 Oracle Database Exception Audit Event

Source Event	Event Description	command_ class	target_type
ERROR NETWORK	Network Error	ERROR	NETWORK

Invalid Record Events

Invalid record events track audited activity that Oracle AVDF cannot recognize, possibly due to a corrupted audit record.

Table C–8 lists the Oracle Database invalid record audit events and the equivalent Oracle AVDF event.

Table C–8 Oracle Database Invalid Record Audit Event

Source Event	Event Description	command_ class	target_type
INVALID RECORD	Invalid Record	INVALID	RECORD

Object Management Events

Object management events track audited actions performed on database objects, such as CREATE TABLE statements.

Table C–9 lists the Oracle Database object management audit events and the equivalent Oracle AVDF events.

Table C–9 Oracle Database Object Management Audit Events

Source Event	Event Description	command_ class	target_type
ALTER DIMENSION	Alter Dimension	ALTER	DIMENSION
ALTER EDITION	Alter Edition (Release 11.2)	ALTER	EDITION
ALTER INDEX	Alter Index	ALTER	INDEX
ALTER MATERIALIZED VIEW	Alter Materialized View	ALTER	MATERIALIZED VIEW
ALTER MATERIALIZED VIEW LOG	Alter Materialized View Log	ALTER	MATERIALIZED VIEW LOG
ALTER MINING MODEL	Alter Mining Model (Release 11.2)	ALTER	MINING MODEL
ALTER OPERATOR	Alter Operator	ALTER	OPERATOR
ALTER OUTLINE	Alter Outline	ALTER	OUTLINE
ALTER PUBLIC SYNONYM	Alter Public Synonym (Release 11.2)	ALTER	PUBLIC SYNONYM
ALTER SEQUENCE	Alter Sequence	ALTER	SEQUENCE
ALTER SYNONYM	Alter Synonym (Release 11.2)	ALTER	SYNONYM
ALTER TABLE	Alter Table	ALTER	TABLE
APPLY TABLE	Apply Table or Schema Policy[1]	APPLY	TABLE
CREATE MINING MODEL	Create Mining Model (Release 11.2)	CREATE	MINING MODEL
CREATE DIMENSION	Create Dimension	CREATE	DIMENSION
CREATE DIRECTORY	Create Directory	CREATE	DIRECTORY

Table C–9 (Cont.) Oracle Database Object Management Audit Events

Source Event	Event Description	command_class	target_type
CREATE EDITION	Create Edition (Release 11.2	CREATE	EDITION
CREATE INDEX	Create Index	CREATE	INDEX
CREATE MATERIALIZED VIEW	Create Materialized View	CREATE	MATERIALIZED VIEW
CREATE MATERIALIZED VIEW LOG	Create Materialized View Log	CREATE	MATERIALIZED VIEW LOG
CREATE OUTLINE	Create Outline	CREATE	OUTLINE
CREATE PUBLIC DATABASE LINK	Create Public Database Link	CREATE	PUBLIC DATABASE LINK
CREATE PUBLIC SYNONYM	Create Public Synonym	CREATE	PUBLIC SYNONYM
CREATE SCHEMA	Create Schema	CREATE	SCHEMA
CREATE SEQUENCE	Create Sequence	CREATE	SEQUENCE
CREATE SYNONYM	Create Synonym	CREATE	SYNONYM
CREATE TABLE	Create Table	CREATE	TABLE
CREATE VIEW	Create View	CREATE	VIEW
DROP DIMENSION	Drop Dimension	DROP	DIMENSION
DROP DIRECTORY	Drop Directory	DROP	DIRECTORY
DROP EDITION	Drop Edition (Release 11.2)	DROP	EDITION
DROP INDEX	Drop Index	DROP	INDEX
DROP MATERIALIZED VIEW	Drop Materialized View	DROP	MATERIALIZED VIEW
DROP MATERIALIZED VIEW LOG	Drop Materialized View Log	DROP	MATERIALIZED VIEW LOG
DROP OUTLINE	Drop Outline	DROP	OUTLINE
DROP PUBLIC DATABASE LINK	Drop Public Database Link	DROP	PUBLIC DATABASE LINK
DROP PUBLIC SYNONYM	Drop Public Synonym	DROP	PUBLIC SYNONYM
DROP SEQUENCE	Drop Sequence	DROP	SEQUENCE
DROP SYNONYM	Drop Synonym	DROP	SYNONYM
DROP TABLE	Drop Table	DROP	TABLE
DROP VIEW	Drop View	DROP	VIEW
FLASHBACK TABLE	Flashback Table	RETRIEVE	TABLE
LOCK	Lock	LOCK	NULL

Table C–9 (Cont.) Oracle Database Object Management Audit Events

Source Event	Event Description	command_class	target_type
PURGE INDEX	Purge Index	DROP	INDEX
PURGE TABLE	Purge Table	DROP	TABLE
REMOVE TABLE OR SCHEMA	Remove Table or Schema[2]	DROP	TABLE OR SCHEMA
RENAME	Rename	RENAME	NULL
UNDROP OBJECT	Undrop Object	UNDO	OBJECT
UPDATE INDEXES	Update Indexes	UPDATE	INDEXES
VALIDATE INDEX	Validate Index	VALIDATE	INDEX

[1] APPLY TABLE OR SCHEMA POLICY is an Oracle Label Security audit event.

[2] REMOVE TABLE OR SCHEMA is an Oracle Label Security audit event.

Peer Association Events

Peer association events track database link statements. Table C–10 lists the Oracle Database peer association audit events and the equivalent Oracle AVDF events.

Table C–10 Oracle Database Peer Association Audit Events

Source Event	Event Description	command_class	target_type
CREATE DATABASE LINK	Create Database Link	CREATE	DATABASE LINK
DROP DATABASE LINK	Drop Database Link	DROP	DATABASE LINK

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.

Table C–11 lists the Oracle Database role and privilege management audit events and the equivalent Oracle AVDF events.

Table C–11 Oracle Database Role and Privilege Management Audit Events

Source Event	Event Description	command_class	target_type
ALTER ROLE	Alter Role	ALTER	ROLE
CREATE ROLE	Create Role	CREATE	ROLE
DROP ROLE	Drop Role	DROP	ROLE
GRANT OBJECT	Grant Object	GRANT	OBJECT
GRANT ROLE	Grant Role	GRANT	ROLE
ERROR OBJECT	Object Exists Errors[1]	FAIL	OBJECT
REVOKE OBJECT	Revoke Object	REVOKE	OBJECT
REVOKE ROLE	Revoke Role	REVOKE	ROLE

Table C–11 (Cont.) Oracle Database Role and Privilege Management Audit Events

Source Event	Event Description	command_class	target_type
SET USER	Set User or Program Unit Label[1]	SET	USER
PROGRAM UNIT LABEL		PROGRAM	UNIT LABEL
PRIVILEGED OPERATION	Privileged Operation	EXECUTE	SYSTEM PRIVILEGE
PRIVILEGED ACTION	Privileged Action[1]	PRIVILEGED	ACTION

[1] OBJECT EXISTS ERRORS, SET USER OR PROGRAM UNIT LABEL, and PRIVILEGED ACTION are Oracle Label Security events.

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.

Table C–12 lists the Oracle Database service and application utilization audit events and the equivalent Oracle AVDF events.

Table C–12 Oracle Database Service and Application Utilization Audit Events

Source Event	Event Description	command_class	target_type
CALL METHOD	Call Method	CALL	METHOD
EXECUTE PROCEDURE	Execute Procedure	EXECUTE	PROCEDURE
EXECUTE PL/SQL	PL/SQL Execute	EXECUTE	PL/SQL

System Management Events

System management events track audited system management activity, such as STARTUP and SHUTDOWN operations. Table C–13 lists the Oracle Database system management audit events and the equivalent Oracle AVDF events.

Table C–13 Oracle Database System Management Audit Events

Source Event	Event Description	command_class	target_type
ALTER CLUSTER	Alter Cluster	ALTER	CLUSTER
ALTER DATABASE	Alter Database	ALTER	DATABASE
ALTER FLASHBACK ARCHIVE	Alter Flashback Archive (Release 11.2)	ALTER	FLASHBACK ARCHIVE
ALTER ROLLBACK SEG	Alter Rollback Seg	ALTER	ROLLBACK SEG
ALTER SYSTEM	Alter System	ALTER	SYSTEM
ALTER TABLESPACE	Alter Tablespace	ALTER	TABLESPACE
ANALYZE CLUSTERS	Analyze Cluster	ANALYZE	CLUSTERS
CREATE CLUSTER	Create Cluster	CREATE	CLUSTER

Table C–13 (Cont.) Oracle Database System Management Audit Events

Source Event	Event Description	command_ class	target_type
CREATE CONTROL FIL	Create Control File	CREATE	CONTROL FILE
CREATE DATABASE	Create Database	CREATE	DATABASE
CREATE FLASHBACK ARCHIVE	Create Flashback Archive (Release 11.2)	CREATE	FLASHBACK ARCHIVE
CREATE ROLLBACK SEG	Create Rollback Seg	CREATE	ROLLBACK SEG
CREATE TABLESPACE	Create Tablespace	CREATE	TABLESPACE
DISABLE ALL TRIGGERS	Disable All Triggers	DISABLE	ALL TRIGGERS
DROP CLUSTER	Drop Cluster	DROP	CLUSTER
DROP FLASHBACK ARCHIVE	Drop Flashback Archive (Release 11.2)	DROP	FLASHBACK ARCHIVE
DROP ROLLBACK SEG	Drop Rollback Seg	DROP	ROLLBACK SEG
DROP TABLESPACE	Drop Tablespace	DROP	TABLESPACE
ENABLE ALL TRIGGERS	Enable All Triggers	ENABLE	ALL TRIGGERS
FLASHBACK	Flashback	RETRIEVE	NULL
FLASHBACK DATABASE	Flashback Database	RETRIEVE	DATABASE
PURGE DBA_ RECYCLEBIN	Purge DBA Recycle Bin	DROP	DBA_ RECYCLEBIN
PURGE TABLESPACE	Purge Tablespace	DROP	TABLESPACE
SHUTDOWN	Shutdown	STOP	DATABASE
STARTUP	Startup	START	DATABASE
SUPER USER TRANSACTION CONTROL	Super User Transaction Control (Release 11.2)	TRANSACTION CONTROL	SUPER USER
SUPER USER DDL	Super User DDL	DDL	SUPER USER
SUPER USER DML	Super User DML	DML	SUPER USER
SYSTEM GRANT	System Grant	GRANT	SYSTEM
REVOKE SYSTEM	System Revoke	REVOKE	SYSTEM
TRUNCATE CLUSTER	Truncate Cluster	TRUNCATE	CLUSTER

Unknown or Uncategorized Events

Unknown or uncategorized events track audited activity that cannot be categorized, such as `ALTER SUMMARY` statements.

Table C–14 lists the Oracle Database unknown or uncategorized audit events and the equivalent Oracle AVDF events.

Table C–14 Oracle Database Unknown or Uncategorized Audit Events

Source Event	Event Description	command_ class	target_type
ALTER SUMMARY	Alter Summary	ALTER	SUMMARY
COMMENT	Comment	COMMENT	NULL
CREATE SUMMARY	Create Summary	CREATE	SUMMARY
DROP SUMMARY	Drop Summary	DROP	SUMMARY
NO-OP	No-Op	NO-OP	NO-OP
SUPER USER UNKNOWN	Super User Unknown	UNKNOWN	SUPER USER
UNKNOWN	Unknown	UNKNOWN	UNKNOWN
USER COMMENT	User Comment	COMMENT	USER

User Session Events

User session events track audited authentication events for users who log in to the database.

Table C–15 lists the Oracle Database user session audit events and the equivalent Oracle AVDF events.

Table C–15 Oracle Database User Session Audit Events

Source Event	Event Description	command_ class	target_type
ALTER SESSION	Alter Session	ALTER	SESSION
COMMIT	Commit	COMMIT	NULL
CREATE RESTORE POINT	Create Restore Point	CREATE	RESTORE POINT
CREATE SESSION	Create Session	CREATE	SESSION
DROP RESTORE POINT	Drop Restore Point	DROP	RESTORE POINT
LOGOFF	Logoff	LOGOUT	NULL
LOGOFF BY CLEANUP	Logoff by Cleanup	LOGOFF BY CLEANUP	NULL
LOGON	Logon	LOGIN	NULL
PROXY AUTHENTICATION ONLY	Proxy Authentication Only	PROXY	AUTHENTICATION ONLY
PURGE USER_ RECYCLEBIN	Purge User Recycle Bin	DROP	USER_ RECYCLEBIN
ROLLBACK	Rollback	ROLLBACK	NULL
SAVEPOINT	Savepoint	SAVEPOINT	NULL
REC SESSION	Session Record	MERGE	SESSION RECORD

Table C–15 (Cont.) Oracle Database User Session Audit Events

Source Event	Event Description	command_ class	target_type
SET ROLE	Set Role	SET	ROLE
SET TRANSACTION	Set Transaction	SET	TRANSACTION
SUPER USER LOGON	Super User Logon	LOGON	SUPER USER

D

Sybase ASE Audit Events

Topics

About the Sybase ASE Audit Events

This appendix maps audit event names used in Sybase Adaptive Server Enterprise (ASE) to their equivalent values in the **command_class** and **target_type** fields in the Oracle AVDF audit record. The audit events are organized in useful categories, for example, Account Management events. You can use the audit events mapped here to create custom audit reports using other Oracle Database reporting products or third-party tools. See also "Oracle Audit Vault and Database Firewall Database Schemas" on page A-1 for Oracle AVDF data warehouse details that may be useful in designing your own reports.

Account Management Events

Account management events track Transact-SQL commands that affect user accounts, such as the `UNLOCK ADMIN ACCOUNT` command. Table D–1 lists the Sybase ASE account management events and the equivalent Oracle AVDF events.

Table D–1 Sybase ASE Account Management Audit Events

Source Event	Event Description	command_class	target_type
CREATE LOGIN COMMAND	Create Login Command	CREATE	USER
DROP LOGIN COMMAND	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
LOGIN HAS BEEN LOCKED	Login Has Been Locked	LOCK	ACCOUNT

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.

Table D–2 lists the Sybase ASE application management events and the equivalent Oracle AVDF events.

Table D–2 Sybase ASE Application Management Audit Events

Source Event	Event Description	command_ class	target_type
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

Audit Command Events

Audit command events track the use of auditing Transact-SQL commands on other Transact-SQL commands and on database objects. Table D–3 lists the Sybase ASE audit command events and the equivalent Oracle AVDF events.

Table D–3 Sybase ASE Audit Command Audit Events

Source Event	Event Description	command_class	target_type
AUDITING DISABLED	Auditing Disabled	NOAUDIT	SERVER
AUDITING ENABLED	Auditing Enabled	AUDIT	SERVER

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 "Data Access Report" on page 6-17, uses these events.

Table D–4 lists the Sybase ASE data access events and the equivalent Oracle AVDF events.

Table D–4 Sybase ASE Data Access Audit Events

Source Event	Event Description	command_ class	target_type
ACCESS TO AUDIT TABLE	Access To Audit Table	ACCESS	TABLE
BCP IN	BCP In	INSERT	TABLE
DELETE TABLE	Delete Table	DELETE	TABLE
DELETE VIEW	Delete View	DELETE	VIEW
INSERT TABLE	Insert Table	INSERT	TABLE
INSERT VIEW	Insert View	INSERT	VIEW
SELECT TABLE	Select Table	SELECT	TABLE
SELECT VIEW	Select View	SELECT	VIEW
TRUNCATE TABLE	Truncate Table	TRUNCATE	TABLE
TRUNCATION OF AUDIT TABLE	Truncation of Audit Table	TRUNCATE	TABLE
UPDATE TABLE	Update Table	UPDATE	TABLE
UPDATE VIEW	Update View	UPDATE	VIEW

Exception Events

Exception events track audited error and exception activity, such as network errors. Table D–5 lists Sybase ASE exception events and the equivalent Oracle AVDF events.

Table D–5 Sybase ASE Exception Audit Events

Source Event	Event Description	command_ class	target_type
FATAL ERROR	Fatal Error	RAISE	ERROR
NONFATAL ERROR	Nonfatal Error	RAISE	ERROR

Invalid Record Events

Invalid record events track audited activity that Oracle AVDF cannot recognize, possibly due to a corrupted audit record.

Object Management Events

Object management events track audited actions performed on database objects, such as CREATE TABLE commands. Table D–6 lists the Sybase ASE object management events and the equivalent Oracle AVDF events.

Table D–6 Sybase ASE Object Management Audit Events

Source Event	Event Description	command_class	target_type
ACCESS TO DATABASE	Access To Database	ACCESS	DATABASE
ALTER TABLE	Alter Table	ALTER	TABLE
BIND DEFAULT	Bind Default	BIND	DEFAULT
BIND MESSAGE	Bind Message	BIND	MESSAGE
BIND RULE	Bind Rule	BIND	RULE
BUILT-IN FUNCTION	Access Database	ACCESS	DATABASE
	Access Object		OBJECT
	Access Schema		SCHEMA
	Access User		USER
	Access Password		PASSWORD
CREATE INDEX	Create Index	CREATE	INDEX
CREATE TABLE	Create Table	CREATE	TABLE
CREATE VIEW	Create View	CREATE	VIEW
CREATION OF REFERENCES TO TABLES	Creation of References to Tables	ASSOCIATE	TABLE
DROP INDEX	Drop Index	DROP	INDEX
DROP TABLE	Drop Table	DROP	TABLE
DROP VIEW	Drop View	DROP	VIEW
TRANSFER TABLE	Transfer Table	MOVE	TABLE
UNBIND DEFAULT	Unbind Default	UNBIND	DEFAULT
UNBIND MESSAGE	Unbind Message	UNBIND	MESSAGE
UNBIND RULE	Unbind Rule	UNBIND	RULE

Peer Association Events

Peer association events track database link commands. These events do not have any event names.

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. Table D–7 lists the Sybase ASE role and privilege management events and the equivalent Oracle AVDF events.

Table D–7 Sybase ASE Role and Privilege Management Audit Events

Source Event	Event Description	command_ class	target_type
GRANT COMMAND	Grant Command	GRANT	OBJECT
REVOKE COMMAND	Revoke Command	REVOKE	OBJECT
ROLE CHECK PERFORMED	Role Check Performed	VALIDATE	ROLE

Table D–7 (Cont.) Sybase ASE Role and Privilege Management Audit Events

Source Event	Event Description	command_ class	target_type
ROLE LOCK	Role Lock	LOCK	ROLE
ROLE TOGGLING	Role Toggling	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

Service and Application Utilization Events

Service and application utilization events track audited application access activity, such as the execution of Transact-SQL commands.

Table D–8 lists the Sybase ASE service and application utilization events and the equivalent Oracle AVDF events.

Table D–8 Sybase ASE Service and Application Utilization Audit Events

Source Event	Event Description	command_ class	target_type
AD HOC AUDIT RECORD	Ad Hoc Audit Record	INSERT	AUDIT RECORD
ALL COMMANDS	All Commands Execution	EXECUTE	COMMAND
EXECUTION OF STORED PROCEDURE	Stored Procedure Execution	EXECUTE	PROCEDURE
EXECUTION OF TRIGGER	Trigger Execution	EXECUTE	TRIGGER
RPC IN	RPC In	REMOTE CALL	PROCEDURE
RPC OUT	RPC Out	REMOTE CALL	PROCEDURE
TRUSTED PROCEDURE EXECUTION	Trusted procedure execution	EXECUTE	PROCEDURE
TRUSTED TRIGGER EXECUTION	Trusted trigger execution	EXECUTE	TRIGGER

System Management Events

System management events track audited system management activity, such as the CREATE DATABASE and DISK INIT commands. Table D–9 lists the Sybase ASE system management events and the equivalent Oracle AVDF events.

Table D–9 Sybase ASE System Management Audit Events

Source Event	Event Description	command_class	target_type
AEK ADD ENCRYPTION	AEK Add Encryption	INSERT	ENCRYPTION KEY
AEK DROP ENCRYPTION	AEK Drop Encryption	DROP	ENCRYPTION KEY
AEK KEY RECOVERY	AEK Key Recovery	RECOVER	ENCRYPTION KEY
AEK MODIFY ENCRYPTION	AEK Modify Encryption	UPDATE	ENCRYPTION KEY
AEK MODIFY OWNER	AEK Modify Owner	UPDATE	OWNER
ALTER DATABASE	Alter Database	ALTER	DATABASE
ALTER ENCRYPTION KEY	Alter Encryption Key	ALTER	ENCRYPTION KEY
ALTER...MODIFY OWNER	Alter Modify Owner	UPDATE	OWNER
AUDIT OPTION CHANGE	Audit Option Change	UPDATE	AUDIT OPTION
CONFIG	Config	CONFIGURE	SYSTEM
CREATE DATABASE	Create Database	CREATE	DATABASE
CREATE ENCRYPTION KEY	Create Encryption Key	CREATE	ENCRYPTION KEY
CREATE MANIFEST FILE	Create Manifest File	CREATE	MANIFEST FILE
DBCC COMMAND	DB Consistency Check	VALIDATE	DATABASE
DEPLOY UDWS	Deploy UDWS	ALTER	SYSTEM
DEPLOY USER-DEFINED WEB SERVICES	Deploy User-Defined Web Services	INSTALL	WEB SERVICE
DISK INIT	Disk Init	INITIALIZE	DISK
DISK MIRROR	Disk Mirror	COPY	DISK
DISK REFIT	Disk Refit	REFRESH	DISK
DISK REINIT	Disk Reinit	INITIALIZE	DISK
DISK RELEASE	Disk Release	RELEASE	DISK
DISK REMIRROR	Disk Remirror	RESUME	DISK
DISK RESIZE	Disk Resize	UPDATE	SYSTEM
DISK UNMIRROR	Disk Unmirror	SUSPEND	DISK
DROP DATABASE	Drop Database	DROP	DATABASE
DROP ENCRYPTION KEY	Drop Encryption Key	DROP	ENCRYPTION KEY
DUMP DATABASE	Dump Database	BACKUP	DATABASE
DUMP TRANSACTION	Dump Transaction	BACKUP	TRANSACTION
ENCRYPTED COLUMN ADMINISTRATION	Encrypted Column Administration	CONFIGURE	ENCRYPTION
ERRORLOG ADMINISTRATION	Errorlog Administration	CONFIGURE	ERROR LOG

Table D–9 (Cont.) Sybase ASE System Management Audit Events

Source Event	Event Description	command_ class	target_type
JCS INSTALL COMMAND	JCS Install Command	INSTALL	JCS
JCS REMOVE COMMAND	JCS Remove Command	UNINSTALL	JCS
KILL/TERMINATE COMMAND	Kill/Terminate Command	ABORT	COMMAND
LDAP STATE CHANGES	LDAP State Changes	UPDATE	LDAP STATE
LOAD DATABASE	Load Database	LOAD	DATABASE
LOAD TRANSACTION	Load Transaction	LOAD	TRANSACTION
MOUNT DATABASE	Mount Database	MOUNT	DATABASE
ONLINE DATABASE	Online Database	PUBLISH	DATABASE
PASSWORD ADMINISTRATION	Password Administration	CONFIGURE	PASSWORD POLICY
QUIESCE DATABASE COMMAND	Quiesce Database Command	QUIESCE	DATABASE
QUIESCE HOLD SECURITY	Quiesce Hold Security	SUSPEND	QUIESCE
QUIESCE RELEASE	Quiesce Release	RESUME	QUIESCE
REGENERATE KEYPAIR	Regenerate Keypair	CREATE	KEYPAIR
SERVER BOOT	Server Boot	STARTUP	DATABASE
SERVER SHUTDOWN	Server Shutdown	SHUTDOWN	DATABASE
SSL ADMINISTRATION	SSL Administration	CONFIGURE	SSL
UNDEPLOY UDWS	Undeploy UDWS	ALTER	SYSTEM
UNDEPLOY USER DEFINED WEB SERVICES	Undeploy User Defined Web Services	UNINSTALL	WEB SERVICE
UNMOUNT DATABASE	Unmount Database	UNMOUNT	DATABASE

Unknown or Uncategorized Events

Unknown or uncategorized events track audited activity that cannot be categorized. Table D–10 shows the Sybase ASE unknown or uncategorized event and the equivalent Oracle AVDF event.

Table D–10 Sybase ASE Unknown or Uncategorized Audit Events

Source Event	Event Description	command_ class	target_ type
AD HOC AUDIT RECORD	Ad Hoc Audit record	UNKNOWN	NULL

User Session Events

User session events track audited authentication events for users who log in to the database.

Table D–11 lists the Sybase ASE user session events and the equivalent Oracle AVDF events.

Table D–11 Sybase ASE User Session Audit Events

Source Event	Event Description	command_ class	target_ type
CONNECT TO COMMAND	Connect to command	CONNECT	CIS
LOG IN	Log In	LOGIN	SERVER
LOG OUT	Log Out	LOGOUT	SERVER
SETUSER COMMAND	Setuser Command	SET	USER

E

Microsoft SQL Server SQL Trace Audit Events

Topics

About the Microsoft SQL Server Audit Events

This appendix maps audit event names used in the SQL Server database to their equivalent values in the **command_class** and **target_type** fields in the Oracle AVDF audit record. The audit events are organized in useful categories, for example, Account Management events. You can use the audit events mapped here to create custom audit reports using other Oracle Database reporting products or third-party tools. See also "Oracle Audit Vault and Database Firewall Database Schemas" on page A-1 for Oracle AVDF data warehouse details that may be useful in designing your own reports.

Account Management Events

Account management events track SQL statements that affect user accounts, such as adding logins or changing login passwords.

Table E–1 lists the Microsoft SQL Server account management events and the equivalent Oracle AVDF events.

Table E–1 SQL Server Account Management Events

Source Event	Event Description	command_class	target_type
ADDLOGIN:ADD	Audit AddLogin Event	CREATE	USER
ADDLOGIN:DROP		DROP	USER
DATABASE PRINCIPAL MANAGEMENT:ALTER: USER	Audit Database Principal Management Event	ALTER	Any from List 1
DATABASE PRINCIPAL MANAGEMENT:CREATE: USER		CREATE	
DATABASE PRINCIPAL MANAGEMENT:DROP: USER		DROP	
LOGIN CHANGE PASSWORD:PASSWORD CHANGED	Audit Login Change Password Event	ALTER	Any from List 1
LOGIN CHANGE PASSWORD:PASSWORD MUST CHANGE		ALTER	
LOGIN CHANGE PASSWORD:PASSWORD RESET		ALTER	
LOGIN CHANGE PASSWORD:PASSWORD SELF CHANGED		ALTER	
LOGIN CHANGE PASSWORD:PASSWORD SELF RESET		ALTER	
LOGIN CHANGE PASSWORD:PASSWORD UNLOCKED		ALTER	
LOGIN CHANGE PROPERTY:CREDENTIAL CHANGED	Audit Login Change Property Event	ALTER	Any from List 1
LOGIN CHANGE PROPERTY:DEFAULT DATABASE		ALTER	
LOGIN CHANGE PROPERTY:DEFAULT DATABASE CHANGED		ALTER	
LOGIN CHANGE PROPERTY:DEFAULT LANGUAGE		ALTER	
LOGIN CHANGE PROPERTY:DEFAULT LANGUAGE CHANGED		ALTER	
LOGIN CHANGE PROPERTY:EXPIRATION CHANGED		ALTER	
LOGIN CHANGE PROPERTY:NAME CHANGED		ALTER	
LOGIN CHANGE PROPERTY:POLICY CHANGED		ALTER	
SERVER OBJECT MANAGEMENT:CREDENTIAL MAP DROPPED	Audit Server Object Management Event	ALTER	USER
SERVER OBJECT MANAGEMENT:CREDENTIAL MAPPED TO LOGIN		ALTER	USER
SERVER PRINCIPAL MANAGEMENT:CREATE	Audit Server Principal Management Event	ALTER	USER
SERVER PRINCIPAL MANAGEMENT:ALTER		CREATE	USER
SERVER PRINCIPAL MANAGEMENT:DROP		DISABLE	Any from List 1
SERVER PRINCIPAL MANAGEMENT:DISABLE		DROP	Any from List 1
SERVER PRINCIPAL MANAGEMENT:ENABLE		ENABLE	Any from List 1

Application Management Events

Application management events track actions that were performed on the underlying SQL statements, such as creating objects.

Table E–2 lists the Microsoft SQL Server application management events and the equivalent Oracle AVDF events.

Table E–2 SQL Server Application Management Audit Events

Source Event	Event Description	command_ class	target_type
DATABASE OBJECT TAKE OWNERSHIP	Audit Database Object Take Ownership Event	ALTER	Any from List 1
SCHEMA OBJECT TAKE OWNERSHIP: OBJECT	Audit Schema Object Take Ownership Event	ALTER	Any from List 1
SCHEMA OBJECT TAKE OWNERSHIP: PROCEDURE		ALTER	
SCHEMA OBJECT TAKE OWNERSHIP: TYPE		ALTER	
SCHEMA OBJECT TAKE OWNERSHIP: TRIGGER		ALTER	
SERVER OBJECT TAKE OWNERSHIP: OBJECT	Audit Server Object Take Ownership Event	ALTER	Any from List 1
OBJECT:CREATED:PROCEDURE	Object:Created	CREATE	Any from List 1
OBJECT:CREATED:TRIGGER		CREATE	
OBJECT:CREATED:TYPE			
OBJECT:CREATED:BEGIN		CREATE	
OBJECT:CREATED:COMMIT		COMMIT	
OBJECT:CREATED:ROLLBACK		ROLLBACK	
OBJECT:DELETED:BEGIN	Object:Deleted	DROP	
OBJECT:DELETED:PROCEDURE	Object:Deleted	DROP	Any from List 1
OBJECT:DELETED:TRIGGER		DROP	

Audit Command Events

Audit command events track the use of audit events, such as altering trace events. Table E–3 lists the Microsoft SQL Server audit command events and the equivalent Oracle AVDF events.

Table E–3 SQL Server Audit Command Audit Events

Source Event	Event Description	command_ class	target_type
CHANGE:AUDIT STARTED	Audit Change Audit Event	AUDIT	Any from List 1
CHANGE:AUDIT STOPPED		NOAUDIT	
CHANGE:C2 MODE ON		AUDIT	
CHANGE:C2 MODE OFF		NOAUDIT	
CHANGE:AUDIT STOPPED		SYSTEM	
CHANGE:NEW AUDIT STARTED		SYSTEM	
SERVER ALTER TRACE	Audit Server Alter Trace Event	ALTER	TRACE
EXISTINGCONNECTION	ExistingConnection	EXISTING	Any from List 1

Table E–4 lists the Microsoft SQL Server audit command events that are logged in the Windows Event Viewer.

Table E–4 SQL Server Audit Command Events Logged in Windows Event Viewer

Source Event	Severity
OP ALTER TRACE: START	10
OP ALTER TRACE: STOP	10

Data Access Events

The data access event tracks SQL transactions. The Data Access Report, described in "Data Access Report" on page 6-17, uses these events.

Table E–5 shows the Microsoft SQL Server data access source event and the equivalent Oracle AVDF event.

Table E–5 SQL Server Data Access Audit Event

Source Event	Event Description	command_ class	target_type
SQL TRANSACTION:BEGIN	SQL Transaction	TRANSACTION MANAGEMENT	TRANSACTION

Exception Events

Exception events track audited error and exception activity, such as background job errors. Table E–6 lists the Microsoft SQL Server exception events and the equivalent Oracle AVDF events.

Table E–6 SQL Server Exception Audit Events

Source Event	Event Description	command _class	target_type
BACKGROUND JOB ERROR:BACKGROUND JOB GIVING UP AFTER FAILURE	Background Job Error	RAISE	Any from List 1
BACKGROUND JOB ERROR:BACKGROUND JOB DROPPED - QUEUE IS FULL		RAISE	
BACKGROUND JOB ERROR:BACKGROUND JOB RETURNED AN ERROR		RAISE	
BLOCKED PROCESS REPORT	Blocked Process Report	RAISE	Any from List 1

Table E–7 lists the Microsoft SQL Server exception events that are logged in the Windows Event Viewer.

Table E–7 SQL Server Exception Events Logged in the Windows Event Viewer

Source Event	Severity	command_ class	target_type
OP ERROR: COMMIT	10	ERROR	Any from List 1
OP ERROR: DB OFFLINE	10	ERROR	Any from List 1
OP ERROR: MIRRORING ERROR	16	ERROR	Any from List 1
OP ERROR: .NET FATAL ERROR	16	ERROR	Any from List 1
OP ERROR: .NET USER CODE	16	ERROR	Any from List 1
OP ERROR: PROCESS VIOLATION	16	ERROR	Any from List 1

Table E–7 (Cont.) SQL Server Exception Events Logged in the Windows Event Viewer

Source Event	Severity	command_ class	target_type
OP ERROR: RECOVER	21	ERROR	Any from List 1
OP ERROR: RESTORE FAILED	21	ERROR	Any from List 1
OP ERROR: ROLLBACK	10	ERROR	Any from List 1
OP ERROR: SERVER SHUT DOWN	21	ERROR	Any from List 1
OP ERROR: STACK OVER FLOW	16	ERROR	Any from List 1

Invalid Record Events

Invalid record events track audited activity that Oracle AVDF cannot recognize, possibly due to a corrupted audit record. These events do not have any event names; they only contain event attributes.

Object Management Events

Object management events track audited actions performed on database objects, such as altering an object. Table E–8 lists the Microsoft SQL Server object management events and the equivalent Oracle AVDF events.

Table E–8 SQL Server Object Management Audit Events

Source Event	Event Description	command_ class	target_type
DATABASE OBJECT ACCESS	Audit Database Object Access Event	ACCESS	Any from List 1
DATABASE OBJECT MANAGEMENT:ACCESS	Audit Database Object Management Event	ACCESS	Any from List 1
DATABASE OBJECT TAKE OWNERSHIP: OBJECT	Audit Database Object Take Ownership Event	ALTER	Any from List 1
DATABASE OBJECT TAKE OWNERSHIP: SCHEMA		ALTER	
DATABASE PRINCIPAL MANAGEMENT:CREATE	Audit Database Principal Management Event	CREATE	Any from List 1
DATABASE PRINCIPAL MANAGEMENT:ALTER		ALTER	
DATABASE PRINCIPAL MANAGEMENT:DROP		DROP	
SCHEMA OBJECT ACCESS	Audit Schema Object Access Event	ACCESS	Any from List 1
SCHEMA OBJECT MANAGEMENT:CREATE	Audit Schema Object Management Event	CREATE	Any from List 1
SCHEMA OBJECT MANAGEMENT:ALTER		ALTER	
SCHEMA OBJECT MANAGEMENT:DROP		DROP	
SCHEMA OBJECT MANAGEMENT:TRANSFER		TRANSFER	
SCHEMA OBJECT TAKE OWNERSHIP: INDEX	Audit Schema Object Take Ownership Event	ALTER	Any from List 1
SCHEMA OBJECT TAKE OWNERSHIP: OBJECT		ALTER	
SCHEMA OBJECT TAKE OWNERSHIP: TABLE		ALTER	
SERVER OBJECT TAKE OWNERSHIP: OBJECT	Audit Server Object Take Ownership Event	ALTER	Any from List 1
LOCK:DEADLOCK	Lock:Deadlock	DEADLOCK	Any from List 1

Table E–8 (Cont.) SQL Server Object Management Audit Events

Source Event	Event Description	command_class	target_type
LOCK:DEADLOCK CHAIN	Lock:Deadlock Chain	DEADLOCK	Any from List 1
LOCK:DEADLOCK CHAIN:RESOURCE TYPE LOCK		DEADLOCK	
OBJECT:ALTERED	Object:Altered	ALTER	Any from List 1
OBJECT:ALTERED:COMMIT		COMMIT	
OBJECT:ALTERED:INDEX		ALTER	
OBJECT:ALTERED:PROCEDURE		ALTER	
OBJECT:ALTERED:ROLLBACK		ROLLBACK	
OBJECT:ALTERED:TABLE		ALTER	
OBJECT:ALTERED:TRIGGER		ALTER	
OBJECT:ALTERED:TYPE		ALTER	
OBJECT:ALTERED:BEGIN		ALTER	
OBJECT:CREATED	Object:Created	CREATE	Any from List 1
OBJECT:CREATED:COMMIT		COMMIT	
OBJECT:CREATED:INDEX		CREATE	
OBJECT:CREATED:PROCEDURE		CREATE	
OBJECT:CREATED:ROLLBACK		ROLLBACK	
OBJECT:CREATED:SCHEMA		CREATE	
OBJECT:CREATED:SYNONYM		CREATE	
OBJECT:CREATED:TABLE		CREATE	
OBJECT:CREATED:TRIGGER		CREATE	
OBJECT:CREATED:TYPE		CREATE	
OBJECT:CREATED:VIEW		CREATE	
OBJECT:DELETED	Object:Deleted	DROP	Any from List 1
OBJECT:DELETED:COMMIT		COMMIT	
OBJECT:DELETED:INDEX		DROP	
OBJECT:DELETED:PROCEDURE		DROP	
OBJECT:DELETED:ROLLBACK		ROLLBACK	
OBJECT:DELETED:SYNONYM		DROP	
OBJECT:DELETED:TABLE		DROP	
OBJECT:DELETED:TRIGGER		DROP	
OBJECT:DELETED:TYPE		DROP	
OBJECT:DELETED:VIEW		DROP	

Peer Association Events

Peer association events track database link statements. These events do not have any event names; they only contain event attributes.

Role and Privilege Management Events

Role and privilege management events track audited role and privilege management activity, such as granting a user access permission.

Table E–9 lists the Microsoft SQL Server role and privilege management events and the equivalent Oracle AVDF events.

Table E–9 SQL Server Role and Privilege Management Audit Events

Source Event	Event Description	command_ class	target_type
ADD DB USER:ADD	Audit Add DB User Event	ALTER	DATABASE
ADD DB USER:DROP		ALTER	DATABASE
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
ADD LOGIN TO SERVER ROLE:ADD	Audit Add Login to Server Role Event	GRANT	ROLE
ADD LOGIN TO SERVER ROLE:DROP		REVOKE	ROLE
ADD MEMBER TO DB ROLE:ADD	Audit Add Member to DB Role Event	GRANT	ROLE
ADD MEMBER TO DB ROLE:CHANGE GROUP		ALTER	ROLE
ADD MEMBER TO DB ROLE:DROP		REVOKE	ROLE
ADD ROLE:ADD	Audit Add Role Event	CREATE	ROLE
ADD ROLE:DROP		DROP	ROLE
APP ROLE CHANGE PASSWORD	Audit App Role Change Password Event	ALTER	Any from List 1
DATABASE OBJECT GDR:DENY	Audit Database Object GDR Event	ALTER	Any from List 1
DATABASE OBJECT GDR:GRANT		ALTER	
DATABASE OBJECT GDR:REVOKE		ALTER	
DATABASE PRINCIPAL MANAGEMENT:ALTER: ROLE	Audit Database Principal Management Event	ALTER	Any from List 1
DATABASE PRINCIPAL MANAGEMENT:CREATE: ROLE		CREATE	
DATABASE PRINCIPAL MANAGEMENT:DROP: ROLE		DROP	
LOGIN GDR:DENY	Audit Login GDR Event	DENY	Any from List 1
LOGIN GDR:GRANT		GRANT	
LOGIN GDR:REVOKE		REVOKE	
OBJECT DERIVED PERMISSION:CREATE	Audit Object Derived Permission Event	CREATE	Any from List 1
OBJECT DERIVED PERMISSION:ALTER		ALTER	
OBJECT DERIVED PERMISSION:DROP		DROP	
OBJECT DERIVED PERMISSION:DUMP		BACKUP	
OBJECT DERIVED PERMISSION:LOAD		RESTORE	
SCHEMA OBJECT GDR:GRANT	Audit Schema Object GDR Event	GRANT	OBJECT
SCHEMA OBJECT GDR:REVOKE		REVOKE	OBJECT
SCHEMA OBJECT GDR:DENY		DENY	OBJECT
OBJECT PERMISSION	Audit Object Derived Permission Event	CHECK	Any from List 1
SERVER OBJECT GDR:GRANT	Audit Server Object GDR Event	ALTER	Any from List 1
SERVER OBJECT GDR:REVOKE		ALTER	
SERVER OBJECT GDR:DENY		ALTER	

Table E–9 (Cont.) SQL Server Role and Privilege Management Audit Events

Source Event	Event Description	command_ class	target_type
SERVER SCOPE GDR:DENY	Audit Server Scope GDR Event	DENY	Any from List 1
SERVER SCOPE GDR:GRANT		GRANT	
SERVER SCOPE GDR:REVOKE		REVOKE	
DATABASE SCOPE GDR:GRANT	Audit Database Scope GDR Event	GRANT	Any from List 1
STATEMENT GDR:REVOKE		REVOKE	
STATEMENT GDR:DENY		DENY	
STATEMENT PERMISSION	Audit Statement Permission Event	VALIDATE	Any from List 1

Service and Application Utilization Events

Service and application utilization events track audited application access activity.

Table E–10 lists the Microsoft SQL Server service and application utilization events and the equivalent Oracle AVDF events.

Table E–10 SQL Server Service and Application Utilization Audit Events

Source Event	Event Description	command_ class	target_type
BROKER CONVERSATION:INVALID SIGNATURE	Audit Broker Conversation	EXECUTE	Any from List 1
BROKER CONVERSATION:NO CERTIFICATE			
BROKER CONVERSATION:NO SECURITY HEADER			
BROKER CONVERSATION:RUN AS TARGET FAILURE			
BROKER:MESSAGE UNDELIVERABLE:SEQUENCED	Broker:Message Undeliverable	TRANSACTION MANAGEMENT	MESSAGE
BROKER:MESSAGE UNDELIVERABLE:UNSEQUENCED	Broker:Message Undeliverable	TRANSACTION MANAGEMENT	MESSAGE
BROKER:MESSAGE UNDELIVERABLE:CORRUPTED MESSAGE	Broker:Corrupted Message	RECEIVE	Any from List 1
BROKER:ACTIVATION:ABORTED	Broker:Activation - The activation stored procedure exited with an error.	ABORT	Any from List 1
BROKER:QUEUE DISABLED	Broker:Queue Disabled	DISABLE	Any from List 1

System Management Events

System management events track audited system management activity, such as backup and restore operations. Table E–11 lists the Microsoft SQL Server system management events and the equivalent Oracle AVDF events.

Table E–11 SQL Server System Management Audit Events

Source Event	Event Description	command_ class	target_type
ADD DB USER:ADD	Audit Add DB User Event	ALTER	DATABASE
ADD DB USER:DROP		ALTER	DATABASE
ADD DB USER:SP_ADDUSER		ALTER	DATABASE
ADD DB USER:SP_DROPUSER		ALTER	DATABASE
BACKUP/RESTORE:BACKUP	Audit Backup/Restore Event	BACKUP	Any from List 1
BACKUP/RESTORE:BACKUPLOG		BACKUP	
BACKUP/RESTORE:RESTORE		RESTORE	
CHANGE DATABASE OWNER	Audit Change Database Owner	ALTER	Any from List 1
DATABASE MANAGEMENT:ALTER	Audit Database Management Event	ALTER	Any from List 1
DATABASE MANAGEMENT:CREATE		CREATE	
DATABASE MANAGEMENT:DROP		DROP	
DATABASE MANAGEMENT:DUMP		BACKUP	
DATABASE MANAGEMENT:LOAD		RESTORE	
DATABASE OBJECT MANAGEMENT:ALTER	Audit Database Object Management Event	ALTER	Any from List 1
DATABASE OBJECT MANAGEMENT:CREATE		ALTER	
DATABASE OBJECT MANAGEMENT:DROP		ALTER	
DATABASE OBJECT MANAGEMENT:DUMP		BACKUP	
DATABASE OBJECT MANAGEMENT:LOAD		RESTORE	
DATABASE OBJECT MANAGEMENT:OPEN		ALTER	
DATABASE OPERATION:SUBSCRIBE TO QUERY NOTIFICATION	Audit Database Operation Event	SUBSCRIBE	Any from List 1
DATABASE PRINCIPAL MANAGEMENT:DUMP	Audit Database Principal Management Event	BACKUP	Any from List 1
DATABASE PRINCIPAL MANAGEMENT:LOAD		RESTORE	
DB CONSISTENCY CHECK	Audit DBCC Event	VERIFY	Any from List 1
SCHEMA OBJECT MANAGEMENT:DUMP	Audit Schema Object Management Event	BACKUP	Any from List 1
SCHEMA OBJECT MANAGEMENT:LOAD		RESTORE	
SERVER OBJECT MANAGEMENT:CREATE	Audit Server Object Management Event	ALTER	SYSTEM
SERVER OBJECT MANAGEMENT:ALTER		ALTER	SYSTEM
SERVER OBJECT MANAGEMENT:DROP		ALTER	SYSTEM
SERVER OBJECT MANAGEMENT:DUMP		BACKUP	Any from List 1
SERVER OBJECT MANAGEMENT:LOAD		RESTORE	Any from List 1
SERVER OPERATION:ADMINISTER BULK OPERATIONS	Audit Server Operation Event	UPDATE	Any from List 1
SERVER OPERATION:ALTER RESOURCES		UPDATE	
SERVER OPERATION:ALTER SERVER STATE		UPDATE	
SERVER OPERATION:ALTER SETTINGS		UPDATE	
SERVER OPERATION:AUTHENTICATE		UPDATE	
SERVER OPERATION:EXTERNAL ACCESS		UPDATE	
SERVER PRINCIPAL MANAGEMENT:DUMP: USER	Audit Server Principal Management Event	BACKUP	Any from List 1
SERVER PRINCIPAL MANAGEMENT:LOAD: USER		RESTORE	

Table E–11 (Cont.) SQL Server System Management Audit Events

Source Event	Event Description	command_class	target_type
SERVER STARTS AND STOPS:SHUTDOWN	Audit Server Starts and Stops	STOP	Any from List 1
SERVER STARTS AND STOPS:STARTED		START	
SERVER STARTS AND STOPS:PAUSED		SUSPEND	
SERVER STARTS AND STOPS:CONTINUE		RESUME	
SERVER STARTS AND STOPS:INSTANCE CONTINUED	Audit Server Starts and Stops Event	RESUME	Any from List 1
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	UPDATE	Any from List 1
DATABASE MIRRORING CONNECTION:CONNECTING	Database Mirroring Connection	CONNECT	DATABASE
DATABASE MIRRORING CONNECTION:CONNECTED		CONNECT	DATABASE
DATABASE MIRRORING CONNECTION:CONNECT FAILED		INVALID	DATABASE
DATABASE MIRRORING CONNECTION:CLOSING		CLOSE	DATABASE
DATABASE MIRRORING CONNECTION:CLOSED		CLOSE	DATABASE
DATABASE MIRRORING CONNECTION:ACCEPT		ACCEPT	DATABASE
DATABASE MIRRORING CONNECTION:SEND IO ERROR		RAISE	DATABASE
DATABASE MIRRORING CONNECTION:RECEIVE IO ERROR		RECEIVE	DATABASE
MOUNT TAPE:TAPE MOUNT CANCELLED	Mount Tape	MOUNT	Any from List 1
MOUNT TAPE:TAPE MOUNT COMPLETE		MOUNT	
MOUNT TAPE:TAPE MOUNT REQUEST		MOUNT	

Unknown or Uncategorized Events

Unknown or uncategorized events track audited activity that cannot be categorized, such as user-created configurations.

Table E–12 Uncategorised Events

Source Event	Event Description	command_class	target_type
ATTENTION	Attention	RAISE	Any from List 1
ERROR LOG	ErrorLog	WRITE	Any from List 1
EXCEPTION	Exception	RAISE	Any from List 1
OLEDB ERRORS	OLEDB Errors	RAISE	Any from List 1
EXECUTION WARNINGS:QUERY WAIT	Execution warnings	WAIT	QUERY
EXECUTION WARNINGS:QUERY TIMEOUT	Execution warnings	DML	QUERY
SORT WARNINGS:SINGLE PASS	Sort Warnings	ACCESS	QUERY
SORT WARNINGS:MULTIPLE PASS	Sort Warnings	ACCESS	QUERY
MISSING COLUMN STATISTICS	Missing Column Statistics	ACCESS	Any from List 1
MISSING JOIN PREDICATE	Missing Join Predicate	ACCESS	Any from List 1
SERVER MEMORY CHANGE:INCREASE	Server Memory Change	UPDATE	MEMORY

Table E–12 (Cont.) Uncategorised Events

Source Event	Event Description	command_class	target_type
SERVER MEMORY CHANGE:DECREASE	Server Memory Change	UPDATE	MEMORY
USER ERROR MESSAGE	User Error Message	RAISE	Any from List 1
BITMAP WARNING:DISABLED	Bitmap Warning	RAISE	WARNING
TRACE START	Trace Start	START	Any from List 1
TRACE STOP	Trace Stop	STOP	Any from List 1
SQL:STMTCOMPLETED	SQL:Stmt Completed Event	EXECUTE	Any from List 1
DBCC	Audit DBCC Event	EXECUTE	Any from List 1
SERVER OPERATION:ALTER SERVER STATE	Audit Server Operation Event	UPDATE	Any from List 1
LOCK:DEADLOCK CHAIN:RESOURCE TYPE LOCK	Lock:Deadlock Chain	DEADLOCK	Any from List 1
USER CONFIGURABLE	User Configurable (Event ID:82)	CONFIGURE	Any from List 1
USER CONFIGURABLE	User Configurable (Event ID:83)	CONFIGURE	Any from List 1
USER CONFIGURABLE	User Configurable (Event ID:84)	CONFIGURE	Any from List 1
USER CONFIGURABLE	User Configurable (Event ID:85)	CONFIGURE	Any from List 1
USER CONFIGURABLE	User Configurable (Event ID:86)	CONFIGURE	Any from List 1
USER CONFIGURABLE	User Configurable (Event ID:87)	CONFIGURE	Any from List 1
USER CONFIGURABLE	User Configurable (Event ID:88)	CONFIGURE	Any from List 1
USER CONFIGURABLE	User Configurable (Event ID:89)	CONFIGURE	Any from List 1
USER CONFIGURABLE	User Configurable (Event ID:90)	CONFIGURE	Any from List 1
USER CONFIGURABLE	User Configurable (Event ID:91)	CONFIGURE	Any from List 1
NOTIFICATION SERVICE	Notification Service	RAISE	DATABASE
PASSWORD POLICY	Password Policy	UPDATE	POLICY

User Session Events

User session events track audited authentication events for users who log in to the database.

Table E–13 lists the Microsoft SQL Server user session events and the equivalent Oracle AVDF events.

Table E–13 SQL Server User Session Audit Events

Source Event	Event Description	command_class	target_type
BROKER LOGIN:AUTHENTICATION FAILURE	Audit Broker Login	LOGIN	Any from List 1
BROKER LOGIN:LOGIN SUCCESS		LOGIN	
BROKER LOGIN:LOGIN PROTOCOL ERROR		LOGIN	
BROKER LOGIN:MESSAGE FORMAT ERROR		LOGIN	
BROKER LOGIN:NEGOTIATE FAILURE		LOGIN	
DATABASE MIRRORING LOGIN:LOGIN SUCCESS	Audit Database Mirroring Login Event	LOGIN	Any from List 1
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			
DATABASE OPERATION:CHECKPOINT	Audit Database Operation Event	SAVEPOINT	Any from List 1
DATABASE PRINCIPAL IMPERSONATION	Audit Database Principal Impersonation Event	IMPERSONATION	Any from List 1
LOGIN:NONPOOLED	Audit Login	LOGIN	USER
LOGIN:POOLED	Audit Login	LOGIN	USER
LOGIN:FAILED	Audit Login Failed	LOGIN	Any from List 1
LOGOUT:NONPOOLED	Audit Logout	LOGOUT	USER
LOGOUT:POOLED	Audit Logout	LOGOUT	USER
LOGIN FAILED:NONPOOLED	Login Failed Event	LOGIN	USER
LOGIN FAILED:POOLED	Login Failed Event	LOGIN	USER
SERVER PRINCIPAL IMPERSONATION	Audit Server Principal Impersonation Event	IMPERSONATION	Any from List 1
SQL TRANSACTION:COMMIT	SQL Transaction	COMMIT	Any from List 1
SQL TRANSACTION:ROLLBACK		ROLLBACK	
SQL TRANSACTION:SAVEPOINT		SAVEPOINT	

Target Type Values

Target Type values associated with certain audit events can be any from the following list. See the Audit Event tables in this Appendix for references.

List 1

Possible Target Types
INDEX
PROCEDURE
TRIGGER
TABLE
VIEW

Possible Target Types
CONSTRAINT
DEFAULT
RULE
DATABASE
OBJECT
CATALOG
SCHEMA
CREDENTIAL
EVENT
FUNCTION
ROLE
GROUP
KEY
LOGIN
REMOTE SERVICE BINDING
NOTIFICATION
SYNONYM
SEQUENCE
END POINT
QUEUE
CERTIFICATE
SERVER
ASSEMBLY
PARTITION SCHEME
USER
SERVICE BROKER SERVICE CONTRACT
TYPE
SERVICE BROKER ROUTE
STATISTICS
SERVICE BROKER SERVICE
CERTIFICATE LOGIN
QUERY

F

Microsoft SQL Server SQL Audit and Event Log Events

Topics

SQL Audit Events

SQL Audit Events map server-level, database-level groups of events and individual events. The Audit action items can be individual actions such as `SELECT` operations on a Table, or a group of actions such as `SERVER_PERMISSION_CHANGE_GROUP`.

SQL Audit Events track the following three categories of Events:

- **Server Level:** These actions include server operations, such as management changes, and logon and logoff operations.
- **Database Level:** These actions include data manipulation languages (DML) and Data Definition Language (DDL).
- **Audit Level:** These actions include actions in the auditing process.

Table F–1 SQL Audit Events

Source Event	Event Description	command_class	target_type
`DATABASE_ROLE_MEMBER_CHANGE_GROUP`	Database Role Member Change Group	`ALTER`	Any from List 1
`BACKUP LOG`	Backup Log	`BACKUP`	Any from List 1
`ALTER RESOURCES`	Alter Resources	`ALTER`	Any from List 1
`DELETE`	Delete	`DELETE`	Any from List 1
`BROKER LOGIN`	Broker Login	`LOGIN`	Any from List 1
`LOGOUT GROUP`	Logout Group	`LOGOUT`	Any from List 1
`MUST CHANGE PASSWORD`	Must Change Password	`UPDATE`	Any from List 1
`DROP MEMBER`	Drop Member	`DROP`	Any from List 1
`DENY`	Deny	`DENY`	Any from List 1
`SEND`	Send	`SEND`	Any from List 1
`SELECT`	Select	`SELECT`	Any from List 1
`SERVER_CONTINUE`	Server Continue	`RESUME`	Any from List 1

Table F–1 (Cont.) SQL Audit Events

Source Event	Event Description	command_class	target_type
SERVER OPERATION GROUP	Server Operation Group	EXECUTE	Any from List 1
INSERT	Insert	INSERT	Any from List 1
EXECUTE	Execute	EXECUTE	Any from List 1
SHOW PLAN	Show Plan	EXECUTE	Any from List 1
SUCCESSFUL_LOGIN_GROUP	Successful Login Group	LOGIN	Any from List 1
SERVER_ROLE_MEMBER_ CHANGE_GROUP	Server Role Member Change Group	ALTER	Any from List 1
ALTER TRACE	Alter Trace	ALTER	Any from List 1
CREDENTIAL MAP TO LOGIN	Credential Map to Login	SET	Any from List 1
FULL TEXT	Full Text	EXECUTE	Any from List 1
TRACE AUDIT C2ON	Trace Audit C2On	AUDIT	Any from List 1
BULK ADMIN	Bulk Admin	INSERT	Any from List 1
TRACE AUDIT C2OFF	Trace Audit C2Off	NOAUDIT	Any from List 1
VIEW SERVER STATE	View Server State	EXECUTE	Any from List 1
SCHEMA_OBJECT_ACCESS_ GROUP	Schema Object Access Group	ACCESS	Any from List 1
ALTER CONNECTION	Alter Connection	ALTER	Any from List 1
ALTER SETTINGS	Alter Settings	ALTER	Any from List 1
ALTER SERVER STATE	Alter Server State	ALTER	Any from List 1
EXTERNAL ACCESS ASSEMBLY	External Access Assembly	ACCESS	Any from List 1
OPEN	Open	OPEN	Any from List 1
AUDIT SHUTDOWN ON FAILURE	Audit Shutdown On Failure	NOAUDIT	Any from List 1
AUDIT SESSION CHANGED	Audit Session Changed	AUDIT	Any from List 1
BACKUP_RESTORE_GROUP	Backup Restore Group	RESTORE	Any from List 1
SERVER_OBJECT_OWNERSHIP_ CHANGE_GROUP	Server Object Ownership Change Group	ALTER	Any from List 1
AUTHENTICATE	Authenticate	AUTHENTICATE	Any from List 1
DATABASE_OWNERSHIP_ CHANGE_GROUP	Database Ownership Change Group	ALTER	Any from List 1
REFERENCES	References	ACCESS	Any from List 1
SERVER_STARTED	Server Started	STARTUP	Any from List 1
DATABASE_OBJECT_ OWNERSHIP_CHANGE_GROUP	Database Object Ownership Change Group	ALTER	Any from List 1
SCHEMA_OBJECT_PERMISSION_ CHANGE_GROUP	Schema Object Permission Change Group	ALTER	Any from List 1
IMPERSONATE	Impersonate	PROXY	Any from List 1
CREATE	Create	CREATE	Any from List 1
SERVER_STATE_CHANGE_GROUP	Server State Change Group	ALTER	Any from List 1
TAKE OWNERSHIP	Take Ownership	ALTER	Any from List 1

Table F–1 (Cont.) SQL Audit Events

Source Event	Event Description	command_class	target_type
TRANSFER	Transfer	MOVE	Any from List 1
CHANGE USERS LOGIN AUTO	Change Users Login Auto	ALTER	Any from List 1
ADD MEMBER	Add Member	UPDATE	Any from List 1
VIEW CHANGETRACKING	View ChangeTracking	EXECUTE	Any from List 1
LOGIN FAILED	Login Failed	LOGIN	Any from List 1
DATABASE_PRINCIPAL_ CHANGE_GROUP	Database Principal Change Group	ALTER	Any from List 1
DATABASE_OBJECT_CHANGE_ GROUP	Database Object Change Group	UPDATE	Any from List 1
DATABASE_MIRRORING_LOGIN_ GROUP	Database Mirroring Login Group	LOGIN	Any from List 1
ALTER	Alter	LOGIN	Any from List 1
PASSWORD EXPIRATION	Password Expiration	EXPIRE	Any from List 1
UPDATE	Update	UPDATE	Any from List 1
NAME CHANGE	Name Change	ALTER	Any from List 1
LOGOUT	Logout	LOGOUT	Any from List 1
LOGIN SUCCEEDED	Login Succeeded	LOGIN	Any from List 1
DATABASE_CHANGE_GROUP	Database Change Group	UPDATE	Any from List 1
LOGIN_CHANGE_PASSWORD_ GROUP	Login Change Password Group	UPDATE	Any from List 1
RESET OWN PASSWORD	Reset Own Password	RESET	Any from List 1
CHANGE USERS LOGIN	Change Users Login	ALTER	Any from List 1
TRACE_CHANGE_GROUP	Trace Change Group	ALTER	Any from List 1
FAILED_LOGIN_GROUP	Failed Login Group	LOGIN	Any from List 1
TRACE AUDIT STOP	Trace Audit Stop	NOAUDIT	Any from List 1
REVOKE	Revoke	REVOKE	Any from List 1
CHANGE OWN PASSWORD	Change Own Password	UPDATE	Any from List 1
CHANGE LOGIN CREDENTIAL	Change Login Credential	ALTER	Any from List 1
RECEIVE	Receive	GET	Any from List 1
AUDIT_CHANGE_GROUP	Audit Change Group	AUDIT	Any from List 1
CHANGE DEFAULT LANGUAGE	Change Default Language	ALTER	Any from List 1
CHANGE PASSWORD	Change Password	UPDATE	Any from List 1
RESTORE	Restore	RESTORE	Any from List 1
DATABASE MIRRORING LOGIN	Database Mirroring Login	LOGIN	Any from List 1
REVOKE WITH CASCADE	Revoke with Cascade	REVOKE	Any from List 1
DROP	Drop	DROP	Any from List 1
SERVER_OBJECT_CHANGE_ GROUP	Server Object Change Group	ALTER	Any from List 1
VIEW_DATABASE_STATE	View Database State	EXECUTE	Any from List 1

Table F–1 (Cont.) SQL Audit Events

Source Event	Event Description	command_class	target_type
SERVER_PRINCIPAL_CHANGE_GROUP	Server Principal Change Group	ALTER	Any from List 1
UNLOCK ACCOUNT	Unlock Account	UNLOCK	Any from List 1
FULLTEXT_GROUP	Fulltext Group	EXECUTE	Any from List 1
ENABLE	Enable	ENABLE	Any from List 1
PASSWORD POLICY	Password Policy	UPDATE	Any from List 1
REVOKE WITH GRANT	Revoke With Grant	REVOKE	Any from List 1
DATABASE_PRINCIPAL_IMPERSONATION_GROUP	Database Principal Impersonation Group	PROXY	Any from List 1
RESET PASSWORD	Reset Password	RESET	Any from List 1
SUBSCRIBE QUERY NOTIFICATION	Subscribe Query Notification	SUBSCRIBE	Any from List 1
SERVER_PRINCIPAL_IMPERSONATION_GROUP	Server Principal Impersonation Group	PROXY	Any from List 1
APPLICATION_ROLE_CHANGE_PASSWORD_GROUP	Application Role Change Password Group	UPDATE	Any from List 1
TRACE AUDIT START	Trace Audit Start	AUDIT	Any from List 1
DATABASE OBJECT PERMISSION CHANGE GROUP	Database Object Permission Change Group	ALTER	Any from List 1
SERVER PAUSED	Server Paused	PAUSE	Any from List 1
DATABASE_OPERATION_GROUP	Database Operation Group	DML	Any from List 1
ACCESS	Access	ACCESS	Any from List 1
DATABASE_PERMISSION_CHANGE_GROUP	Database Permission Change Group	ALTER	Any from List 1
UNSAFE ASSEMBLY	Unsafe Assembly	ACCESS	Any from List 1
DENY WITH CASCADE	Deny with Cascade	DENY	Any from List 1
DBCC_GROUP	DBCC Group	EXECUTE	Any from List 1
BROKER_LOGIN_GROUP	Broker Login Group	LOGIN	Any from List 1
CHECKPOINT	Checkpoint	SAVEPOINT	Any from List 1
SERVER SHUTDOWN	Server Shutdown	SHUTDOWN	Any from List 1
NO CREDENTIAL MAP TO LOGIN	No Credential Map to Login	SET	Any from List 1
SCHEMA_OBJECT_CHANGE_GROUP	Schema Object Change Group	ALTER	Any from List 1
CONNECT	Connect	CONNECT	Any from List 1
GRANT WITH GRANT	Grant with Grant	GRANT	Any from List 1
CHANGE DEFAULT DATABASE	Change Default Database	ALTER	Any from List 1
DISABLE	Disable	DISABLE	Any from List 1
SCHEMA_OBJECT_OWNERSHIP CHANGE_GROUP	Schema Object Ownership Change Group	ALTER	Any from List 1
GRANT	Grant	GRANT	Any from List 1

Table F–1 (Cont.) SQL Audit Events

Source Event	Event Description	command_class	target_type
SERVER_PERMISSION_CHANGE_GROUP	Server Permission Change Group	ALTER	Any from List 1
SERVER_OBJECT_PERMISSION CHANGE_GROUP	Server Object Permission Change Group	ALTER	Any from List 1
DATABASE_OBJECT_ACCESS_GROUP	Database Object Access Group	ACCESS	Any from List 1
DBCC	DBCC	EXECUTE	Any from List 1
BACKUP	Backup	BACKUP	Any from List 1

Event Log Events

Event Log Events help you audit server-level, database-level and individual events. These events consist of zero or more audit action items which can be either a group of actions (DATABASE_MIRRORING_LOGIN_GROUP) or individual actions (SELECT or REVOKE).

The Event Log Events track the following three categories of events.

- **Server Level**: These actions include server operations such as management changes, and logon and logoff operations.
- **Database Level**: These actions include data manipulation (DML) languages and Data Definition Language (DDL).
- **Audit Level**: These actions include actions in the auditing process.

Table F–2 Event Log Events

Source Events	Event Description	command_class	target_types
OP ALTER TRACE:STOP	OP Alter Trace: Stop	STOP	DATABASE
OP ALTER TRACE:START	OP Alter Trace: Start (Event ID: 19033)	START	DATABASE
OP ALTER TRACE:START	OP Alter Trace: Start (Event ID: 19034)	START	DATABASE
LOGIN FAILED: ONLY ADMINISTRATORS CAN CONNECT AT THIS TIME	Login Failed: Only Administrators Can Connect At This Time (Event ID: 18450)	LOGIN	DATABASE
LOGIN FAILED: ONLY ADMINISTRATORS CAN CONNECT AT THIS TIME	Login Failed: Only Administrators Can Connect At This Time (Event ID: 18451)	LOGIN	DATABASE
LOGIN FAILED: UNTRUSTED DOMAIN	Login Failed: Untrusted Domain	LOGIN	DATABASE
LOGIN SUCCEEDED: TRUSTED	Login Succeeded: Trusted	LOGIN	DATABASE
LOGIN SUCCEEDED: NON-TRUSTED	Login Succeeded: Non-Trusted	LOGIN	DATABASE
LOGIN SUCCEEDED	Login Succeeded	LOGIN	DATABASE
LOGIN FAILED	Login Failed	LOGIN	DATABASE
LOGIN FAILED: ILLEGAL USER NAME	Login Failed: Illegal User Name	LOGIN	DATABASE

Table F–2 (Cont.) Event Log Events

Source Events	Event Description	command_class	target_types
LOGIN FAILED: SIMULTANEOUS LICENSE LIMIT	Login Failed: Simultaneous License Limit	LOGIN	DATABASE
LOGIN FAILED: WORKSTATION LICENSING LIMIT	Login Failed: Workstation Licensing Limit	LOGIN	DATABASE
LOGIN FAILED: SIMULTANEOUS LICENSE LIMIT	Login Failed: Simultaneous License Limit	LOGIN	DATABASE
LOGIN FAILED: SERVER IN SINGLE USER MODE	Login Failed: Server in Single User Mode	LOGIN	DATABASE
LOGIN FAILED: ACCOUNT DISABLED	Login Failed: Account Disabled	LOGIN	DATABASE
LOGIN FAILED: ACCOUNT LOCKED	Login Failed: Account Locked	LOGIN	DATABASE
LOGIN FAILED: PASSWORD EXPIRED	Login Failed: Password Expired	LOGIN	DATABASE
LOGIN FAILED: PASSWORD MUST BE CHANGED	Login Failed: Password Must Be Changed	LOGIN	DATABASE
OP ERROR: SERVER SHUT DOWN	OP Error: Server Shut Down	RAISE	DATABASE
OP ERROR: MIRRORING ERROR	OP Error: Mirroring Error	RAISE	DATABASE
OP ERROR: STACK OVER FLOW	OP Error: Stack Over Flow	RAISE	DATABASE
OP ERROR: COMMIT	OP Error: Commit	RAISE	DATABASE
OP ERROR: ROLLBACK	OP Error: Rollback	RAISE	DATABASE
OP ERROR: DB OFFLINE	OP Error: DB Offline	RAISE	DATABASE
OP ERROR: PROCESS VIOLATION	OP Error: Process Violation	RAISE	DATABASE
OP ERROR: RESTORE FAILED	OP Error: Restore Failed	RAISE	DATABASE
OP ERROR: RECOVER	OP Error: Recover	RAISE	DATABASE
OP ERROR: .NET FATAL ERROR	OP Error: .NET Fatal Error	RAISE	DATABASE
OP ERROR: .NET USER CODE	OP Error: .NET User Code	RAISE	DATABASE
NOTIFICATION SERVICE	Notification Service	RAISE	DATABASE
PASSWORD POLICY UPDATE SUCCESFUL	Password Policy Update Successful	UPDATE	POLICY
OP modify: START	OP Modify: Start	STARTUP	DATABASE
OP modify: STOP	OP Modify: Stop	SHUTDOWN	DATABASE

Target Type Values

Target Type values associated with certain audit events can be any from the following list. See the Audit Event tables in this Appendix for references.

List 1

Possible Target Types	Class_Type
CONSTRAINT	F
DATABASE	DT

Possible Target Types	Class_Type
DATABASE	DN
KEY	DK
CONSTRAINT	UQ
USER	US
CATALOG	FC
ENDPOINT	EP
NOTIFICATION	EN
VIEW	V
TYPE	TY
TREE	XR
FUNCTION	FS
FUNCTION	FT
FUNCTION	FN
STOPLIST	FL
USER	WU
GROUP	WG
USER	WL
STORED PROCEDURE	X
USER	GU
RESOURCE	RG
FILTER	RF
ROLE	RL
TABLE	S
ASSEMBLY	AS
ROLE	AR
QUERY	AQ
USER	AU
CONSTRAINT	C
QUERY	PQ
BROKER PRIORITY	PR
PARTITION	PS
AGGREGATE	AF
KEY	AK
USER	AL
RULE	R
Undocumented	AP
FUNCTION	TF
DEFAULT	D

Possible Target Types	Class_Type
TRIGGER	TR
USER	SU
SERVICE	SV
STATISTICS	ST
SCHEMA	SX
SERVICE	BN
TABLE	U
ASSEMBLY	TA
SERVER	SD
SCHEMA	SC
SESSION	SE
ROLE	SG
USER	CU
CONTRACT	CT
USER	SL
DATABASE	DB
KEY	SK
AUDIT SPECIFICATION	DA
SYNONYM	SN
SERVER	SR
QUEUE	SQ
ROUTE	RT
CREDENTIAL	CD
CERTIFICATE	CR
SERVER	CO
PROVIDER	CP
SERVER	T
AUDIT SPECIFICATION	SA
USER	CL
USER	LX
KEY	MK
MESSAGE	MT
OBJECT	ON
OBJECT	OB
STORED PROCEDURE	P
PRIMARY KEY	PK
FUNCTION	PF
ASSEMBLY	PC

Possible Target Types	Class_Type
SERVER AUDIT	A
FUNCTION	IF
FUNCTION	IS
TABLE	IT
INDEX	IX

G

IBM DB2 Audit Events

Topics

About the IBM DB2 for LUW Audit Events

This appendix maps audit event names used in IBM DB2 for LUW to their equivalent values in the **command_class** and **target_type** fields in the Oracle AVDF audit record. The audit events are organized in useful categories, for example, Account Management events. You can use the audit events mapped here to create custom audit reports using other Oracle Database reporting products or third-party tools. See also "Oracle Audit Vault and Database Firewall Database Schemas" on page A-1 for Oracle AVDF data warehouse details that may be useful in designing your own reports.

Account Management Events

Account management events track SQL commands that affect user accounts, such as the `UNLOCK ADMIN ACCOUNT` command. Table G–1 lists the IBM DB2 account management events and the equivalent Oracle AVDF events.

Table G–1 IBM DB2 Account Management Audit Events

Source Event	Event Description	command_ class	target_type
ADD_DEFAULT_ROLE	Add Default Role	CREATE	NULL
ADD_USER	Add User	CREATE	Any from List 3
ALTER_USER_ADD_ROLE	Alter User Add Role	ALTER	NULL
ALTER_USER_ADD_ROLE	Alter User Add Role	ALTER	Any from List 3
ALTER_USER_ AUTHENTICATION	Alter User Authentication	ALTER	Any from List 3
ALTER_USER_DROP_ROLE	Alter User Drop Role	ALTER	Any from List 3
AUTHENTICATION	Authentication	VALIDATE	NULL
DROP_DEFAULT_ROLE	Drop Default Role	DROP	NULL
DROP_USER	Drop User	DROP	Any from List 3
SET_SESSION_USER	Set Session User	SET	Any from List 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.

Table G–2 lists the IBM DB2 application management events and the equivalent Oracle AVDF events.

Table G–2 IBM DB2 Application Management Audit Events

Source Event	Event Description	command_ class	target_type
ALTER_OBJECT	Alter Object	ALTER	Any from List 2
		ALTER	
		ALTER	
		ALTER	
		ALTER	
		ALTER	
CREATE_OBJECT	Create Object	CREATE	Any from List 2
		CREATE	
		CREATE	
		CREATE	
		CREATE	
		CREATE	
DROP_OBJECT	Drop Object	DROP	Any from List 2
		DROP	
		DROP	
		DROP	
		DROP	
		DROP	

Audit Command Events

Audit command events track the use of auditing SQL commands on other SQL commands and on database objects. Table G–3 lists the IBM DB2 audit command events and the equivalent Oracle AVDF events.

Table G–3 IBM DB2 Audit Command Audit Events

Source Event	Event Description	command_ class	target_type
ALTER_AUDIT_POLICY	Alter Audit Policy	AUDIT	POLICY
ARCHIVE	Archive	ARCHIVE	NULL
AUDIT_REMOVE	Audit Remove	NOAUDIT	NULL
AUDIT_REPLACE	Audit Replace	AUDIT	NULL
AUDIT_USING	Audit Using	AUDIT	NULL
CONFIGURE	Configure	AUDIT	NULL
CREATE_AUDIT_POLICY	Create Audit Policy	AUDIT	POLICY
DROP_AUDIT_POLICY	Drop Audit Policy	NOAUDIT	POLICY
PRUNE	Prune	GRANT	NULL
START	Start	AUDIT	NULL
STOP	Stop	NOAUDIT	NULL

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 "Data Access Report" on page 6-17, uses these events.

Table G–4 lists the IBM DB2 data access events and the equivalent Oracle AVDF events.

Table G–4 IBM DB2 Data Access Audit Events

Source Event	Event Description	command_class	target_type
EXECUTE	Execute	INSERT UPDATE	NULL
GET_DB_CFG	Get DB Cfg	GET	NULL
GET_DFLT_CFG	Get Dflt Cfg	GET	NULL
GET_GROUPS	Get Groups	GET	NULL
GET_TABLESPACE_ STATISTIC	Get Tablespace Statistic	GET	NULL
GET_USERID	Get Userid	GET	NULL
READ_ASYNC_LOG_ RECORD	Read Async Log Record	READ	NULL
STATEMENT	Statement	SELECT	NULL
STATEMENT	Statement	UPDATE	NULL
STATEMENT	Statement	INSERT	NULL
STATEMENT	Statement	DELETE	NULL

Exception Events

Exception events track audited error and exception activity, such as network errors. These events do not have any event names.

Invalid Record Events

Invalid record events track audited activity that Oracle AVDF cannot recognize, possibly due to a corrupted audit record.

Object Management Events

Object management events track audited actions performed on database objects, such as `CREATE TABLE` commands. Table G–5 lists the IBM DB2 object management events and the equivalent Oracle AVDF events.

Table G–5 IBM DB2 Object Management Audit Events

Source Event	Event Description	command_class	target_type
ALTER_OBJECT	Alter Object	ALTER	Any from List 2
		ALTER	
		ALTER	
		ALTER	
		ALTER	
		ALTER	
CREATE_OBJECT	Create Object	CREATE	Any from List 2
		CREATE	
		CREATE	
		CREATE	
		CREATE	
		CREATE	
DROP_OBJECT	Drop Object	DROP	Any from List 2
		DROP	
		DROP	
		DROP	
		DROP	
		DROP	
RENAME_OBJECT	Rename Object	RENAME	Any from List 2

Peer Association Events

Peer association events track database link commands. These events do not have any event names; they only contain event attributes.

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. Table G–6 lists the IBM DB2 role and privilege management events and the equivalent Oracle AVDF events.

Table G–6 IBM DB2 Role and Privilege Management Audit Events

Source Event	Event Description	command_ class	target_type
ADD_DEFAULT_ROLE	Add Default Role	CREATE	NULL
ALTER_DEFAULT_ROLE	Alter Default Role	ALTER	NULL
ALTER_OBJECT	Alter Object	ALTER	Any from List 2
ALTER SECURITY POLICY	Alter security policy	ALTER	NULL
CHECKING_FUNCTION	Checking Function	VALIDATE	Any from List 1
CHECKING_MEMBERSHIP_IN_ ROLES	Checking Membership In Roles	VALIDATE	NULL
CHECKING_OBJECT	Checking Object	VALIDATE	Any from List 1
CHECKING_TRANSFER	Checking Transfer	VALIDATE	NULL
CREATE_OBJECT	Create Object	CREATE	Any from List 2
DROP_DEFAULT_ROLE	Drop Default Role	DROP	NULL
DROP_OBJECT	Drop Object	DROP	Any from List 2
GRANT	Grant	GRANT	Any from List 3
GRANT_DB_AUTH	Grant DB Auth	GRANT	NULL
GRANT_DB_AUTHORITIES	Grant DB Authorities	GRANT	NULL
GRANT_DBADM	Grant DBADM	GRANT	NULL
IMPLICIT_GRANT	Implicit Grant	GRANT	Any from List 3
IMPLICIT_REVOKE	Implicit Revoke	REVOKE	Any from List 3
REVOKE	Revoke	REVOKE	Any from List 3
REVOKE_DB_AUTH	Revoke DB Auth	REVOKE	NULL
REVOKE_DB_AUTHORITIES	Revoke DB Authorities	SYSTEM	NULL
REVOKE_DBADM	Revoke DBADM	REVOKE	NULL

Service and Application Utilization Events

Service and application utilization events track audited application access activity, such as the execution of SQL commands.

Table G–7 lists the IBM DB2 service and application utilization events and the equivalent Oracle AVDF events.

Table G–7 IBM DB2 Service and Application Utilization Audit Events

Source Event	Event Description	command_ class	target_type
EXECUTE	Execute	EXECUTE	NULL
EXECUTE_IMMEDIATE	Execute Immediate	EXECUTE	NULL
TRANSFER	Transfer	GRANT	NULL

System Management Events

System management events track audited system management activity, such as the CREATE DATABASE and DISK INIT commands. Table G–8 lists the IBM DB2 system management events and the equivalent Oracle AVDF events.

Table G–8 IBM DB2 System Management Audit Events

Source Event	Event Description	command_ class	target_type
ACTIVATE_DB	Activate DB	ALTER	NULL
ADD_NODE	Add Node	CREATE	NULL
ALTER_BUFFERPOOL	Alter Bufferpool	ALTER	NULL
ALTER_DATABASE	Alter Database	ALTER	NULL
ALTER_NODEGROUP	Alter Nodegroup	ALTER	NULL
ALTER_OBJECT	Alter Object	ALTER	Any from List 2
ALTER_TABLESPACE	Alter Tablespace	ALTER	TABLESPACE
BACKUP_DB	Backup DB	BACKUP	DATABASE
BIND	Bind	ALTER	NULL
CATALOG_DB	Catalog DB	SET	NULL
CHANGE_DB_COMMENT	Change DB Comment	UPDATE	NULL
CATALOG_DCS_DB	Catalog Dcs DB	SET	NULL
CATALOG_NODE	Catalog Node	SET	NULL
CHECK_GROUP_MEMBERSHIP	Check Group Membership	VALIDATE	NULL
CLOSE_CONTAINER_QUERY	Close Container Query	CLOSE	NULL
CLOSE_CURSOR	Close Cursor	CLOSE	CURSOR
CLOSE_HISTORY_FILE	Close History File	ALTER	NULL
CLOSE_TABLESPACE_QUERY	Close Tablespace Query	CLOSE	NULL
CONFIGURE	Configure	AUDIT	NULL
CREATE_BUFFERPOOL	Create Bufferpool	CREATE	NULL
CREATE_DATABASE	Create Database	CREATE	DATABASE
CREATE_DB_AT_NODE	Create DB at Node	CREATE	NULL
CREATE_EVENT_MONITOR	Create Event Monitor	CREATE	NULL
CREATE_INSTANCE	Create Instance	CREATE	NULL
CREATE_NODEGROUP	Create Nodegroup	CREATE	NULL
CREATE_OBJECT	Create Object	CREATE	Any from List 2
CREATE_TABLESPACE	Create Tablespace	CREATE	TABLESPACE
DB2AUDIT	DB2 Audit	ALTER	NULL
DB2REMOT	DB2 Remote	REMOTE CALL	NULL
DB2SET	DB2 Set	ALTER	NULL
DB2TRC	Db2trc	DROP	NULL
DBM_CFG_OPERATION	DBM Cfg Operation	CONFIGURE	NULL

Table G–8 (Cont.) IBM DB2 System Management Audit Events

Source Event	Event Description	command_class	target_type
DEACTIVATE_DB	Deactivate DB	ALTER	NULL
DESCRIBE	Describe	DESCRIBE	NULL
DESCRIBE_DATABASE	Describe Database	DESCRIBE	NULL
DELETE_INSTANCE	Delete Instance	DELETE	NULL
DISCOVER	Discover	GET	NULL
DROP_BUFFERPOOL	Drop Bufferpool	DROP	NULL
DROP_DATABASE	Drop Database	DROP	DATABASE
DROP_EVENT_MONITOR	Drop Event Monitor	DROP	NULL
DROP_NODE_VERIFY	Drop Node Verify	DROP	NULL
DROP_NODEGROUP	Drop Nodegroup	DROP	NULL
DROP_OBJECT	Drop Object	DROP	Any from List 2
DROP_TABLESPACE	Drop Tablespace	DROP	NULL
ENABLE_MULTIPAGE	Enable Multipage	ENABLE	NULL
EXTERNAL_CANCEL	External Cancel	STOP	NULL
ESTIMATE_SNAPSHOT_SIZE	Estimate Snapshot Size	CALCULATE	NULL
EXTRACT	Extract	GET	NULL
FETCH_CONTAINER_QUERY	Fetch Container Query	RETRIEVE	NULL
FETCH_CURSOR	Fetch Cursor	RETRIEVE	CURSOR
FETCH_HISTORY_FILE	Fetch History File	RETRIEVE	NULL
FETCH_TABLESPACE	Fetch Tablespace	RETRIEVE	NULL
FETCH_TABLESPACE_QUERY	Fetch Tablespace Query	RETRIEVE	NULL
FLUSH	Flush	FLUSH	NULL
FORCE_APPLICATION	Force Application	FORCE	NULL
GET_SNAPSHOT	Get Snapshot	GET	NULL
GET_USERMAPPING_FROM_PLUGIN	Get Usermapping From Plugin	GET	NULL
IMPLICIT_REBIND	Implicit Rebind	BIND	NULL
KILLDBM	Kill DBM	ALTER	NULL
LIST_DRDA_INDOUBT_TRANSACTIONS	List Drda Indoubt Transactions	LIST	NULL
LIST_LOGS	List Logs	LIST	NULL
LOAD_MSG_FILE	Load Msg File	LOAD	NULL
LOAD_TABLE	Load Table	INSERT	NULL
MERGE_DBM_CONFIG_FILE	Merge DBM Config File	UPDATE	NULL
MIGRATE_DB	Migrate DB	MIGRATE	NULL
MIGRATE_DB_DIR	Migrate DB DIR	MIGRATE	NULL
MIGRATE_SYSTEM_DIRECTORY	Migrate System Directory	MIGRATE	NULL

Table G–8 (Cont.) IBM DB2 System Management Audit Events

Source Event	Event Description	command_class	target_type
OPEN_CONTAINER_QUERY	Open Container Query	OPEN	NULL
OPEN_CURSOR	Open Cursor	OPEN	CURSOR
OPEN_HISTORY_FILE	Open History File	OPEN	NULL
OPEN_TABLESPACE_QUERY	Open Tablespace Query	OPEN	NULL
PREPARE	Prepare	ASSIGN	NULL
PRUNE_RECOVERY_HISTORY	Prune Recovery History	PRUNE	NULL
QUIESCE_TABLESPACE	Quiesce Tablespace	ALTER	NULL
REBIND	Rebind	ALTER	NULL
REDISTRIBUTE	Redistribute	SEND	NULL
REDISTRIBUTE_NODEGROUP	Redistribute Nodegroup	SEND	NULL
RELEASE SAVEPOINT	Release savepoint	RELEASE	NULL
RENAME_TABLESPACE	Rename Tablespace	RENAME	NULL
RESET_ADMIN_CFG	Reset Admin Cfg	RESET	NULL
RESET_DB_CFG	Reset DB Cfg	RESET	NULL
RESET_DBM_CFG	Reset DBM Cfg	RESET	NULL
RESET_MONITOR	Reset Monitor	RESET	NULL
RESTORE_DB	Restore DB	RESTORE	DATABASE
ROLLFORWARD_DB	Rollforward DB	ROLLFORWARD	DATABASE
RUNSTATS	Run Stats	EXECUTE	NULL
SAVEPOINT	Savepoint	SAVEPOINT	NULL
SET_APPL_PRIORITY	Set Appl Priority	SET	NULL
SET_EVENT_MONITOR_STATE	Set Event Monitor State	SET	NULL
SET_MONITOR	Set Monitor	SET	NULL
SET_RUNTIME_DEGREE	Set Runtime Degree	SET	NULL
SET SAVEPOINT	Set Savepoint	SET	NULL
SET_TABLESPACE_CONTAINERS	Set Tablespace Containers	SET	NULL
SINGLE_TABLESPACE_QUERY	Single Tablespace Query	EXECUTE	NULL
START_DB2	Start DB2	STARTUP	DATABASE
STOP_DB2	Stop DB2	SHUTDOWN	DATABASE
UNCATALOG_DB	Uncatalog DB	RESET	NULL
UNLOAD_TABLE	Unload Table	DELETE	NULL
UNQUIESCE_TABLESPACE	Unquiesce Tablespace	ALTER	NULL
UPDATE_ADMIN_CFG	Update Admin Cfg	UPDATE	NULL
UPDATE_AUDIT	Update Audit	ALTER	NULL
UPDATE_CLI_CONFIGURATION	Update CLI Configuration	UPDATE	NULL
UPDATE_DB_CFG	Update DB Cfg	UPDATE	NULL

Table G–8 (Cont.) IBM DB2 System Management Audit Events

Source Event	Event Description	command_class	target_type
UPDATE_DB_VERSION	Update DB Version	UPDATE	NULL
UNCATALOG_DCS_DB	Uncatalog Dcs DB	RESET	NULL
UNCATALOG_NODE	Uncatalog Node	RESET	NULL
UPDATE_DBM_CFG	Update DBM Cfg	UPDATE	Any from List 3
UPDATE_RECOVERY_HISTORY	Update Recovery History	UPDATE	NULL

Unknown or Uncategorized Events

Unknown or uncategorized events track audited activity that cannot be categorized. Table G–9 lists the IBM DB2 unknown or uncategorized event and equivalent Oracle AVDF event.

Table G–9 IBM DB2 Unknown or Uncategorized Audit Events

Source Event	Event Description	command_class	target_type
ALTER_OBJECT	Alter Object	ALTER	Any from List 2
CREATE_OBJECT	Create Object	CREATE	Any from List 2
DROP_OBJECT	Drop Object	DROP	Any from List 2

User Session Events

User session events track audited authentication events for users who log in to the database.

Table G–10 lists the IBM DB2 user session events and the equivalent Oracle AVDF events.

Table G–10 IBM DB2 User Session Audit Events

Source Event	Event Description	command_class	target_type
ATTACH	Attach	CONNECT	NULL
AUTHENTICATE	Authenticate	AUTHENTICATE	NULL
COMMIT	Commit	COMMIT	NULL
CONNECT	Connect	LOGIN	NULL
CONNECT_RESET	Connect Reset	LOGOUT	NULL
CONNECT RESET	Connect Reset	LOGOUT	NULL
DETACH	Detach	DISCONNECT	NULL
GLOBAL COMMIT	Global Commit	COMMIT	NULL
GLOBAL ROLLBACK	Global Rollback	ROLLBACK	NULL
REQUEST_ROLLBACK	Request Rollback	REQUEST	NULL
ROLLBACK	Rollback	ROLLBACK	NULL

Table G–10 (Cont.) IBM DB2 User Session Audit Events

Source Event	Event Description	command_ class	target_type
SET_SESSION_USER	Set Session User	SET	NULL
SWITCH_USER	Switch User	MOVE	NULL
SWITCH USER	Switch User	MOVE	NULL

Target Type Values

Target Type values associated with certain audit events can be any from the following lists. See the Audit Event tables in the appendix for references.

List 1

Possible Target Types
SYNONYM
ALL
POLICY
BUFFERPOOL
DATABASE
EVENT MONITOR
FUNCTION
FUNCTION MAPPING
VARIABLE
HISTOGRAM TEMPLATE
INDEX
INSTANCE
METHOD
MODULE
NODEGROUP
NONE
PROFILE
PACKAGE
PACKAGE CACHE
REOPT VALUES
ROLE
SCHEMA
SEQUENCE
SERVER
SERVER OPTION
SERVICE CLASS

Possible Target Types
PROCEDURE
TABLE
TABLESPACE
THRESHOLD
CONTEXT
TYPE MAPPING
TYPE&TRANSFORM
USER MAPPING
VIEW
WORK ACTION SET
WORK CLASS SET
WORKLOAD
WRAPPER
XSR OBJECT

List 2

Possible Target Types
SYNONYM
POLICY
BUFFERPOOL
CONSTRAINT
TYPE
EVENT MONITOR
FOREIGN_KEY
FUNCTION
FUNCTION MAPPING
GLOBAL_VARIABLE
HISTOGRAM TEMPLATE
INDEX
INDEX EXTENSION
JAVA
METHOD
MODULE
NODEGROUP
NONE
PACKAGE
PRIMARY_KEY

Possible Target Types
ROLE
SCHEMA
LABEL
SECURITY LABEL COMPONENT
POLICY
SEQUENCE
SERVER
SERVER OPTION
SERVICE CLASS
PROCEDURE
TABLE
TABLESPACE
THRESHOLD
TRIGGER
CONTEXT
TYPE MAPPING
TYPE&TRANSFORM
CONSTRAINT
USER MAPPING
VIEW
WORK ACTION SET
WORK CLASS SET
WORKLOAD
WRAPPER

List 3

Possible Target Types
RULE
DATABASE
FUNCTION
VARIABLE
INDEX
METHOD
MODULE
SYNONYM
NONE
PACKAGE

Possible Target Types
ROLE
SCHEMA
LABEL
POLICY
SERVER
PROCEDURE
TABLE
TABLESPACE
CONTEXT
VIEW
WORKLOAD
XSR OBJECT

H

MySQL Audit Events

This appendix maps audit event names used in MySQL to their equivalent values in the **command_class** and **target_type** fields in the Oracle AVDF audit record. You can use the audit events mapped here to create custom audit reports using other Oracle Database reporting products or third-party tools. See also "Oracle Audit Vault and Database Firewall Database Schemas" on page A-1 for Oracle AVDF data warehouse details that may be useful in designing your own reports.

Table H–1 lists the MySQL audit events and the equivalent Oracle AVDF events.

Table H–1 MySQL Audit Events

Source Event	command_class	target_type
AUDIT	AUDIT	No Mapping
BINLOG DUMP	DUMP	No Mapping
CHANGE USER	CHANGE	No Mapping
CLOSE STMT	CLOSE	No Mapping
CONNECT OUT	CONNECT	No Mapping
CONNECT	CONNECT	No Mapping
CREATE DB	CREATE	No Mapping
DAEMON	DAEMON	No Mapping
DEBUG	DEBUG	No Mapping
DELAYED INSERT	INSERT	No Mapping
DROP DB	DROP	No Mapping
EXECUTE	EXECUTE	No Mapping
FETCH	FETCH	No Mapping
FIELD LIST	LIST	No Mapping
INIT DB	INIT	No Mapping
KILL	KILL	No Mapping
LONG DATA	LONG DATA	No Mapping
NOAUDIT	NOAUDIT	No Mapping
PING	PING	No Mapping
PREPARE	PREPARE	No Mapping
PROCESSLIST	PROCESS	No Mapping

Table H–1 (Cont.) MySQL Audit Events

Source Event	command_class	target_type
QUERY	QUERY	No Mapping
QUIT	QUIT	No Mapping
REFRESH	REFRESH	No Mapping
REGISTER SLAVE	REGISTER	No Mapping
RESET STMT	RESET	No Mapping
SET OPTION	SET	No Mapping
SHUTDOWN	SHUTDOWN	No Mapping
SLEEP	SLEEP	No Mapping
STATISTICS	STATISTICS	No Mapping
TABLE DUMP	DUMP	No Mapping
TIME	TIME	No Mapping

Solaris Operating System Audit Events

This appendix maps audit event names used in the Solaris Operating System to their equivalent values in the **command_class** and **target_type** fields in the Oracle AVDF audit record. You can use the audit events mapped here to create custom audit reports using other Oracle Database reporting products or third-party tools. See also "Oracle Audit Vault and Database Firewall Database Schemas" on page A-1 for Oracle AVDF data warehouse details that may be useful in designing your own reports.

Table I–1 lists the Solaris audit events and the equivalent Oracle AVDF events.

Table I–1 Solaris Audit Events

Source Event	command_class	target_type
AUE_AT_CREATE	CREATE	AT JOB
AUE_AT_DELETE	DELETE	AT JOB
AUE_AUDITON_SETSMASK	SET	AUDIT SESSION
AUE_NDMP_RESTORE	RESTORE	BACKUP LOCATION
AUE_RSHD	EXECUTE	COMMAND
AUE_PROCESSOR_BIND	BIND	CPU
AUE_P_ONLINE	CONTROL	CPU
AUE_CRON_INVOKE	EXECUTE	CRON JOB
AUE_CRONTAB_CREATE	CREATE	CRON JOB
AUE_CRONTAB_DELETE	DELETE	CRON JOB
AUE_CRONTAB_MOD	SET	CRON JOB
AUE_IOCTL	CONTROL	DEVICE
AUE_ATTACH	MOUNT	DEVICE
AUE_DA_ALLOCATE	ALLOCATE	DEVICE
AUE_DA_ALLOCATE_FORCED	ALLOCATE	DEVICE
AUE_DA_DEALLOCATE	DEALLOCATE	DEVICE
AUE_DA_DEALLOCATE_FORCED	DEALLOCATE	DEVICE
AUE_DA_LIST_DEVICES	LIST	DEVICE
AUE_DETACH	UNMOUNT	DEVICE
AUE_REMOVE	EJECT	DEVICE
AUE_SMSERVERD	CONTROL	DEVICE

Table I–1 (Cont.) Solaris Audit Events

Source Event	command_class	target_type
AUE_TPM_CERTIFYSELFTEST	CONTROL	DEVICE
AUE_TPM_CONTINUESELFTEST	CONTROL	DEVICE
AUE_TPM_DISABLEFORCECLEAR	CONTROL	DEVICE
AUE_TPM_DISABLEOWNERCLEAR	CONTROL	DEVICE
AUE_TPM_FIELDUPGRADE	CONTROL	DEVICE
AUE_TPM_FORCECLEAR	CONTROL	DEVICE
AUE_TPM_OWNERCLEAR	CONTROL	DEVICE
AUE_TPM_OWNERSETDISABLE	CONTROL	DEVICE
AUE_TPM_PHYSICALDEACTIVATE	CONTROL	DEVICE
AUE_TPM_PHYSICALDISABLE	CONTROL	DEVICE
AUE_TPM_PHYSICALENABLE	CONTROL	DEVICE
AUE_TPM_PHYSICALPRESENCE	CONTROL	DEVICE
AUE_TPM_RESETLOCKVALUE	CONTROL	DEVICE
AUE_TPM_SELFTESTFULL	CONTROL	DEVICE
AUE_TPM_SETOPERATORAUTH	CONTROL	DEVICE
AUE_TPM_SETOWNERINSTALL	CONTROL	DEVICE
AUE_TPM_SETTEMPDEACTIVATED	CONTROL	DEVICE
AUE_TPM_TAKEOWNERSHIP	CONTROL	DEVICE
AUE_MKDIR	CREATE	DIRECTORY
AUE_RMDIR	DELETE	DIRECTORY
AUE_FT_MKDIR	CREATE	DIRECTORY
AUE_FT_RMDIR	DELETE	DIRECTORY
AUE_DOORFS_DOOR_CALL	EXECUTE	DOOR HANDLER
AUE_DOORFS_DOOR_CREATE	CREATE	DOOR HANDLER
AUE_DOORFS_DOOR_RETURN	EXIT	DOOR HANDLER
AUE_DOORFS_DOOR_REVOKE	DELETE	DOOR HANDLER
AUE_ACCESS	CHECK	FILE
AUE_ACLSET	CONTROL	FILE
AUE_CHMOD	SET	FILE
AUE_CHOWN	SET	FILE
AUE_CLOSE	CLOSE	FILE
AUE_CREAT	CREATE	FILE
AUE_EXEC	EXECUTE	FILE
AUE_EXECVE	EXECUTE	FILE
AUE_FACCESSAT	CHECK	FILE
AUE_FACLSET	SET	FILE
AUE_FCHMOD	SET	FILE

Table I–1 (Cont.) Solaris Audit Events

Source Event	command_class	target_type
AUE_FCHOWN	SET	FILE
AUE_FCHOWNAT	SET	FILE
AUE_FCNTL	CONTROL	FILE
AUE_FSTATAT	GET	FILE
AUE_FSTATFS	GET	FILE
AUE_FUSERS	GET	FILE
AUE_FUTIMESAT	SET	FILE
AUE_INST_SYNC	WRITE	FILE
AUE_LCHOWN	SET	FILE
AUE_LSTAT	GET	FILE
AUE_MMAP	MAP	FILE
AUE_OPENAT_R	OPEN	FILE
AUE_OPENAT_RC	OPEN	FILE
AUE_OPENAT_RT	OPEN	FILE
AUE_OPENAT_RTC	OPEN	FILE
AUE_OPENAT_RW	OPEN	FILE
AUE_OPENAT_RWC	OPEN	FILE
AUE_OPENAT_RWT	OPEN	FILE
AUE_OPENAT_RWTC	OPEN	FILE
AUE_OPENAT_W	OPEN	FILE
AUE_OPENAT_WC	OPEN	FILE
AUE_OPENAT_WT	OPEN	FILE
AUE_OPENAT_WTC	OPEN	FILE
AUE_OPEN_E	OPEN	FILE
AUE_OPEN_R	OPEN	FILE
AUE_OPEN_RC	OPEN	FILE
AUE_OPEN_RT	OPEN	FILE
AUE_OPEN_RTC	OPEN	FILE
AUE_OPEN_RW	OPEN	FILE
AUE_OPEN_RWC	OPEN	FILE
AUE_OPEN_RWT	OPEN	FILE
AUE_OPEN_RWTC	OPEN	FILE
AUE_OPEN_S	OPEN	FILE
AUE_OPEN_W	OPEN	FILE
AUE_OPEN_WC	OPEN	FILE
AUE_OPEN_WT	OPEN	FILE
AUE_OPEN_WTC	OPEN	FILE

Table I–1 (Cont.) Solaris Audit Events

Source Event	command_class	target_type
AUE_PATHCONF	GET	FILE
AUE_PFEXEC	EXECUTE	FILE
AUE_RENAME	RENAME	FILE
AUE_RENAMEAT	RENAME	FILE
AUE_STAT	CHECK	FILE
AUE_STATFS	CHECK	FILE
AUE_UNLINK	UNLINK	FILE
AUE_UNLINKAT	UNLINK	FILE
AUE_UTIME	SET	FILE
AUE_UTIMES	SET	FILE
AUE_WRITE	WRITE	FILE
AUE_FILE_COPY	COPY	FILE
AUE_FILE_RELABEL	LABEL	FILE
AUE_PRINT_REQUEST	PRINT	FILE
AUE_PRINT_REQUEST_PS	PRINT	FILE
AUE_PRINT_REQUEST_UNLABELED	PRINT	FILE
AUE_PRINT_REQUEST_NOBANNER	PRINT	FILE
AUE_FT_CHMOD	SET	FILE
AUE_FT_CHOWN	SET	FILE
AUE_FT_GET	RECEIVE	FILE
AUE_FT_PUT	SEND	FILE
AUE_FT_REMOVE	DELETE	FILE
AUE_FT_RENAME	RENAME	FILE
AUE_FT_UTIMES	SET	FILE
AUE_NDMP_BACKUP	BACKUP	FILE
AUE_PROF_CMD	EXECUTE	FILE
AUE_SUDO	EXECUTE	FILE
AUE_VSCAN_QUARANTINE	QUARANTINE	FILE
AUE_PORTFS_ASSOCIATE	BIND	FILE PORT
AUE_PORTFS_DISSOCIATE	UNBIND	FILE PORT
AUE_MOUNT	MOUNT	FILE SYSTEM
AUE_STATVFS	CHECK	FILE SYSTEM
AUE_UMOUNT	UNMOUNT	FILE SYSTEM
AUE_UMOUNT2	UNMOUNT	FILE SYSTEM
AUE_MOUNTD_MOUNT	MOUNT	FILE SYSTEM
AUE_MOUNTD_UMOUNT	UNMOUNT	FILE SYSTEM
AUE_UADMIN_REMOUNT	REMOUNT	FILE SYSTEM

Table I–1 (Cont.) Solaris Audit Events

Source Event	command_class	target_type
AUE_UADMIN_SWAPCTL	CONTROL	FILE SYSTEM
AUE_FT_START	OPEN	FILE TRANSFER SESSION
AUE_FT_STOP	CLOSE	FILE TRANSFER SESSION
AUE_HOTPLUG_SET	SET	HOTPLUG CONNECTOR
AUE_HOTPLUG_INSTALL	INSTALL	HOTPLUG PORT
AUE_HOTPLUG_STATE	SET	HOTPLUG PORT
AUE_HOTPLUG_UNINSTALL	UNINSTALL	HOTPLUG PORT
AUE_ILB_CREATE_HEALTHCHECK	CREATE	ILB HEALTHCHECK OBJECT
AUE_ILB_DELETE_HEALTHCHECK	DELETE	ILB HEALTHCHECK OBJECT
AUE_ILB_CREATE_RULE	CREATE	ILB RULE
AUE_ILB_DELETE_RULE	DELETE	ILB RULE
AUE_ILB_DISABLE_RULE	DISABLE	ILB RULE
AUE_ILB_ENABLE_RULE	ENABLE	ILB RULE
AUE_ILB_DISABLE_SERVER	DISABLE	ILB SERVER
AUE_ILB_ENABLE_SERVER	ENABLE	ILB SERVER
AUE_ILB_REMOVE_SERVER	DELETE	ILB SERVER
AUE_ILB_ADD_SERVER	ADD	ILB SERVER GROUP
AUE_ILB_CREATE_SERVERGROUP	CREATE	ILB SERVER GROUP
AUE_ILB_DELETE_SERVERGROUP	DELETE	ILB SERVER GROUP
AUE_INETD_CONNECT	CONNECT	INET SERVICE
AUE_INETD_COPYLIMIT	RESTRICT	INET SERVICE
AUE_INETD_FAILRATE	DISABLE	INET SERVICE
AUE_INETD_RATELIMIT	RESTRICT	INET SERVICE
AUE_PF_POLICY_ADDRULE	ADD	IPSEC POLICY
AUE_PF_POLICY_ALGS	UPDATE	IPSEC POLICY
AUE_PF_POLICY_CLONE	COPY	IPSEC POLICY
AUE_PF_POLICY_DELRULE	DELETE	IPSEC POLICY
AUE_PF_POLICY_FLIP	FLIP	IPSEC POLICY
AUE_PF_POLICY_FLUSH	CLEAR	IPSEC POLICY
AUE_KADMIND_AUTH	EXECUTE	KERBEROS OPERATION
AUE_KADMIND_UNAUTH	EXECUTE	KERBEROS OPERATION
AUE_KRB5KDC_AS_REQ	EXECUTE	KERBEROS SERVICE
AUE_KRB5KDC_TGS_REQ	EXECUTE	KERBEROS SERVICE
AUE_KRB5KDC_TGS_REQ_2NDTKTMM	EXECUTE	KERBEROS SERVICE
AUE_KRB5KDC_TGS_REQ_ALT_TGT	EXECUTE	KERBEROS SERVICE
AUE_MODADDMAJ	BIND	KERNEL MODULE
AUE_MODDEVPLCY	SET	KERNEL MODULE

Table I–1 (Cont.) Solaris Audit Events

Source Event	command_class	target_type
AUE_MODLOAD	LOAD	KERNEL MODULE
AUE_MODUNLOAD	UNLOAD	KERNEL MODULE
AUE_CONFIGKSSL	CONTROL	KERNEL SSL PORT
AUE_LINK	CREATE	LINK
AUE_READLINK	READ	LINK
AUE_FT_SYMLINK	CREATE	LINK
AUE_MEMCNTL	CONTROL	MEMORY
AUE_MUNMAP	UNMAP	MEMORY OBJECT
AUE_MSGCTL	CONTROL	MESSAGE QUEUE
AUE_MSGCTL_RMID	DELETE	MESSAGE QUEUE
AUE_MSGCTL_SET	SET	MESSAGE QUEUE
AUE_MSGCTL_STAT	CHECK	MESSAGE QUEUE
AUE_MSGGET	GET	MESSAGE QUEUE
AUE_MSGRCV	RECEIVE	MESSAGE QUEUE
AUE_MSGSND	SEND	MESSAGE QUEUE
AUE_NDMP_CONNECT	CONNECT	NDMP CLIENT
AUE_NDMP_DISCONNECT	DISCONNECT	NDMP CLIENT
AUE_NETCFG_REMOVE	DELETE	NETCFG PROFILE
AUE_NETCFG_UPDATE	SET	NETCFG PROFILE
AUE_NWAM_DISABLE	DISABLE	NETCFG PROFILE
AUE_NWAM_ENABLE	ENABLE	NETCFG PROFILE
AUE_PIPE	CREATE	PIPE
AUE_AUDITON_GETCAR	GET	PROCESS
AUE_AUDITON_GETCWD	GET	PROCESS
AUE_AUDITON_GETPINFO	GET	PROCESS
AUE_AUDITON_GETPINFO_ADDR	GET	PROCESS
AUE_AUDITON_SETPMASK	SET	PROCESS
AUE_CHDIR	SET	PROCESS
AUE_CHROOT	SET	PROCESS
AUE_CORE	DUMP	PROCESS
AUE_EXIT	EXIT	PROCESS
AUE_FCHDIR	SET	PROCESS
AUE_FCHROOT	SET	PROCESS
AUE_FORK	CREATE	PROCESS
AUE_FORK1	CREATE	PROCESS
AUE_FORKALL	CREATE	PROCESS
AUE_GETAUDIT	GET	PROCESS

Table I–1 (Cont.) Solaris Audit Events

Source Event	command_class	target_type
AUE_GETAUDIT_ADDR	GET	PROCESS
AUE_GETAUID	GET	PROCESS
AUE_KILL	SIGNAL	PROCESS
AUE_NICE	SET	PROCESS
AUE_SETAUDIT	SET	PROCESS
AUE_SETAUDIT_ADDR	SET	PROCESS
AUE_SETAUID	SET	PROCESS
AUE_SETEGID	SET	PROCESS
AUE_SETEUID	SET	PROCESS
AUE_SETGID	SET	PROCESS
AUE_SETGROUPS	SET	PROCESS
AUE_SETPGID	SET	PROCESS
AUE_SETPGRP	SET	PROCESS
AUE_SETPPRIV	SET	PROCESS
AUE_SETREGID	SET	PROCESS
AUE_SETREUID	SET	PROCESS
AUE_SETSID	SET	PROCESS
AUE_SETUID	SET	PROCESS
AUE_SHMAT	BIND	PROCESS
AUE_SHMDT	UNBIND	PROCESS
AUE_SIGQUEUE	SIGNAL	PROCESS
AUE_VFORK	CREATE	PROCESS
AUE_REXD	EXECUTE	RPC
AUE_REXECD	EXECUTE	RPC
AUE_SCREENLOCK	LOCK	SCREEN
AUE_SCREENUNLOCK	UNLOCK	SCREEN
AUE_SEMCTL	CONTROL	SEMAPHORE
AUE_SEMCTL_GETALL	GET	SEMAPHORE
AUE_SEMCTL_RMID	DELETE	SEMAPHORE
AUE_SEMCTL_SET	SET	SEMAPHORE
AUE_SEMCTL_SETALL	SET	SEMAPHORE
AUE_SEMCTL_SETVAL	SET	SEMAPHORE
AUE_SEMCTL_STAT	CHECK	SEMAPHORE
AUE_SEMGET	GET	SEMAPHORE
AUE_SEMOP	CONTROL	SEMAPHORE
AUE_SHMCTL	CONTROL	SHARED MEMORY
AUE_SHMCTL_RMID	UNBIND	SHARED MEMORY

Table I–1 (Cont.) Solaris Audit Events

Source Event	command_class	target_type
AUE_SHMCTL_SET	SET	SHARED MEMORY
AUE_SHMCTL_STAT	CHECK	SHARED MEMORY
AUE_SHMGET	GET	SHARED MEMORY
AUE_SMF_ANNOTATION	ANNOTATE	SMF ACTION
AUE_SMF_MILESTONE	ENABLE	SMF MILESTONE
AUE_SMF_CREATE_PROP	CREATE	SMF PROPERTY
AUE_SMF_CREATE_NPG	CREATE	SMF PROPERTY GROUP
AUE_SMF_CREATE_PG	CREATE	SMF PROPERTY GROUP
AUE_SMF_CLEAR	RESET	SMF SERVICE
AUE_SMF_CREATE	CREATE	SMF SERVICE
AUE_SMF_DEGRADE	DEGRADE	SMF SERVICE
AUE_SMF_DELCUST	DELETE	SMF SERVICE
AUE_SMF_DELETE	DELETE	SMF SERVICE
AUE_SMF_DISABLE	DISABLE	SMF SERVICE
AUE_SMF_ENABLE	ENABLE	SMF SERVICE
AUE_SMF_IMMEDIATE_DEGRADE	DEGRADE	SMF SERVICE
AUE_SMF_IMMEDIATE_MAINTENANCE	MAINTAIN	SMF SERVICE
AUE_SMF_IMMTMP_MAINTENANCE	MAINTAIN	SMF SERVICE
AUE_SMF_MAINTENANCE	MAINTAIN	SMF SERVICE
AUE_SMF_REFRESH	REFRESH	SMF SERVICE
AUE_SMF_REMOVE	DELETE	SMF SERVICE
AUE_SMF_RESTART	RESTART	SMF SERVICE
AUE_SMF_TMP_DISABLE	DISABLE	SMF SERVICE
AUE_SMF_TMP_ENABLE	ENABLE	SMF SERVICE
AUE_SMF_TMP_MAINTENANCE	MAINTAIN	SMF SERVICE
AUE_SMF_UNMASK	UNMASK	SMF SERVICE
AUE_SMF_REMOVE_BUNDLE	DELETE	SMF SERVICE BUNDLE
AUE_SMF_CHANGE_PROP	SET	SMF SERVICE PROPERTY
AUE_SMF_DELCUST_PROP	DELETE	SMF SERVICE PROPERTY
AUE_SMF_DELETE_PROP	DELETE	SMF SERVICE PROPERTY
AUE_SMF_READ_PROP	READ	SMF SERVICE PROPERTY
AUE_SMF_REMOVE_PROP	DELETE	SMF SERVICE PROPERTY
AUE_SMF_UNMASK_PROP	UNMASK	SMF SERVICE PROPERTY
AUE_SMF_DELCUST_PG	DELETE	SMF SERVICE PROPERTY GROUP
AUE_SMF_DELETE_NPG	DELETE	SMF SERVICE PROPERTY GROUP
AUE_SMF_DELETE_PG	DELETE	SMF SERVICE PROPERTY GROUP
AUE_SMF_REMOVE_PG	DELETE	SMF SERVICE PROPERTY GROUP

Table I–1 (Cont.) Solaris Audit Events

Source Event	command_class	target_type
AUE_SMF_UNMASK_PG	UNMASK	SMF SERVICE PROPERTY GROUP
AUE_SMF_ATTACH_SNAP	ATTACH	SMF SNAPSHOT
AUE_SMF_CREATE_SNAP	CREATE	SMF SNAPSHOT
AUE_SMF_DELETE_SNAP	DELETE	SMF SNAPSHOT
AUE_ACCEPT	ACCEPT	SOCKET
AUE_ACCEPT	BIND	SOCKET
AUE_CONNECT	CONNECT	SOCKET
AUE_RECV	RECEIVE	SOCKET
AUE_RECVFROM	RECEIVE	SOCKET
AUE_RECVMSG	RECEIVE	SOCKET
AUE_SEMCTL_GETNCNT	GET	SOCKET
AUE_SEMCTL_GETPID	GET	SOCKET
AUE_SEMCTL_GETVAL	CHECK	SOCKET
AUE_SEMCTL_GETZCNT	CHECK	SOCKET
AUE_SEND	SEND	SOCKET
AUE_SENDMSG	SEND	SOCKET
AUE_SENDTO	SEND	SOCKET
AUE_SETSOCKOPT	SET	SOCKET
AUE_SHUTDOWN	SHUTDOWN	SOCKET
AUE_SOCKACCEPT	ACCEPT	SOCKET
AUE_SOCKCONNECT	CONNECT	SOCKET
AUE_SOCKET	CREATE	SOCKET
AUE_SOCKRECEIVE	RECEIVE	SOCKET
AUE_SOCKSEND	SEND	SOCKET
AUE_SOCKCONFIG	CONTROL	SOCKET NAME
AUE_MKNOD	CREATE	SPECIAL FILE
AUE_GETMSG	READ	STREAM
AUE_GETPMSG	READ	STREAM
AUE_PUTMSG	SEND	STREAM
AUE_PUTPMSG	SEND	STREAM
AUE_SYMLINK	CREATE	SYMBOLIC LINK
AUE_SYSTEMBOOT	BOOT	SYSTEM
AUE_ACCT	CONTROL	SYSTEM PROPERTY
AUE_ADJTIME	SET	SYSTEM PROPERTY
AUE_AUDITON_GETAMASK	GET	SYSTEM PROPERTY
AUE_AUDITON_GETCLASS	GET	SYSTEM PROPERTY
AUE_AUDITON_GETCOND	GET	SYSTEM PROPERTY

Table I–1 (Cont.) Solaris Audit Events

Source Event	command_class	target_type
AUE_AUDITON_GETKAUDIT	GET	SYSTEM PROPERTY
AUE_AUDITON_GETKMASK	GET	SYSTEM PROPERTY
AUE_AUDITON_GETSTAT	GET	SYSTEM PROPERTY
AUE_AUDITON_GPOLICY	GET	SYSTEM PROPERTY
AUE_AUDITON_GQCTRL	GET	SYSTEM PROPERTY
AUE_AUDITON_SETAMASK	SET	SYSTEM PROPERTY
AUE_AUDITON_SETCLASS	SET	SYSTEM PROPERTY
AUE_AUDITON_SETCOND	SET	SYSTEM PROPERTY
AUE_AUDITON_SETKAUDIT	SET	SYSTEM PROPERTY
AUE_AUDITON_SETKMASK	SET	SYSTEM PROPERTY
AUE_AUDITON_SETSTAT	RESET	SYSTEM PROPERTY
AUE_AUDITON_SPOLICY	SET	SYSTEM PROPERTY
AUE_AUDITON_SQCTRL	SET	SYSTEM PROPERTY
AUE_CLOCK_SETTIME	SET	SYSTEM PROPERTY
AUE_CRYPTOADM	CONTROL	SYSTEM PROPERTY
AUE_MODADDPRIV	CONTROL	SYSTEM PROPERTY
AUE_PRIOCNTLSYS	CONTROL	SYSTEM PROPERTY
AUE_SETRLIMIT	SET	SYSTEM PROPERTY
AUE_STIME	SET	SYSTEM PROPERTY
AUE_SYSINFO	CONTROL	SYSTEM PROPERTY
AUE_CPU_ONDEMAND	SET	SYSTEM PROPERTY
AUE_CPU_PERFORMANCE	SET	SYSTEM PROPERTY
AUE_CPU_THRESHOLD	SET	SYSTEM PROPERTY
AUE_UADMIN_CONFIG	SET	SYSTEM PROPERTY
AUE_ENTERPROM	ENTER	SYSTEM RESOURCE
AUE_EXITPROM	EXIT	SYSTEM RESOURCE
AUE_NTP_ADJTIME	SET	SYSTEM RESOURCE
AUE_LABELSYS_TNMLP	CONTROL	TRUSTED NETWORK MULTI-LEVEL PORT
AUE_LABELSYS_TNRH	CONTROL	TRUSTED NETWORK REMOTE HOST
AUE_LABELSYS_TNRHTP	CONTROL	TRUSTED NETWORK REMOTE HOST TEMPLATE
AUE_AUDITON_SETUMASK	SET	USER
AUE_ADMIN_AUTHENTICATE	AUTHENTICATE	USER
AUE_FTPD	LOGON	USER
AUE_FTPD_LOGOUT	LOGOFF	USER
AUE_LOGIN	LOGON	USER
AUE_LOGOUT	LOGOFF	USER

Table I–1 (Cont.) Solaris Audit Events

Source Event	command_class	target_type
AUE_NEWGRP_LOGIN	LOGON	USER
AUE_PASSWD	SET	USER
AUE_RLOGIN	LOGON	USER
AUE_ROLE_LOGIN	LOGON	USER
AUE_ROLE_LOGOUT	LOGOFF	USER
AUE_SMBD_LOGOFF	LOGOFF	USER
AUE_SMBD_SESSION	LOGON	USER
AUE_SSH	LOGON	USER
AUE_SU	LOGON	USER
AUE_SU_LOGOUT	LOGOFF	USER
AUE_TELNET	LOGON	USER
AUE_ZLOGIN	LOGON	USER
AUE_DLADM_CREATE_SECOBJ	CREATE	WIFI SECURITY OBJECT
AUE_DLADM_DELETE_SECOBJ	DELETE	WIFI SECURITY OBJECT
AUE_XCONNECT	CONNECT	X CLIENT
AUE_XDISCONNECT	DISCONNECT	X CLIENT
AUE_POOL_EXPORT	EXPORT	ZFS POOL
AUE_POOL_IMPORT	IMPORT	ZFS POOL
AUE_BRANDSYS	CONTROL	ZONE
AUE_ZONE_STATE	SET	ZONE
AUE_HALT_SOLARIS	SHUTDOWN	
AUE_INIT_SOLARIS	SET	
AUE_POWEROFF_SOLARIS	SHUTDOWN	
AUE_REBOOT_SOLARIS	REBOOT	
AUE_SHUTDOWN_SOLARIS	SHUTDOWN	
AUE_UADMIN_DUMP	DUMP	
AUE_UADMIN_FREEZE	SUSPEND	
AUE_UADMIN_FTRACE	TRACE	
AUE_UADMIN_REBOOT	REBOOT	
AUE_UADMIN_SHUTDOWN	SHUTDOWN	
AUE_UADMIN_THAW	RESUME	

J

Microsoft Windows Operating System Audit Events

This appendix maps audit event names used in the Microsoft Windows Operating System to their equivalent values in the **command_class** and **target_type** fields in the Oracle AVDF audit record. You can use the audit events mapped here to create custom audit reports using other Oracle Database reporting products or third-party tools. See also "Oracle Audit Vault and Database Firewall Database Schemas" on page A-1 for Oracle AVDF data warehouse details that may be useful in designing your own reports.

Table J–1 lists the Windows audit events and the equivalent Oracle AVDF events.

Table J–1 Windows Audit Events

Source Event	command_ class	target_type
ACCOUNT_MAPPED_FOR_LOGON	LOGIN	ACCOUNT
ACCOUNT_COULD_NOT_MAP_FOR_LOGON	LOGIN	ACCOUNT
ATTEMPTED_TO_VALIDATE_ACCOUNT_CREDENTIAL	VALIDATE	ACCOUNT
FAILED_TO_VALIDATE_ACCOUNT_CREDENTIAL	VALIDATE	ACCOUNT
KERBEROS_AUTHENTICATE_TICKET_REQUEST	AUTHENTICATE	SYSTEM
KERBEROS_PRE_AUTHENTICATION_FAILED	AUTHENTICATE	SYSTEM
KERBEROS_AUTHENTICATION_TICKET_REQUEST_FAILED	AUTHENTICATE	SYSTEM
KERBEROS_SERVICE_TICKET_REQUESTED	REQUEST	SYSTEM
KERBEROS_SERVICE_TICKET_RENEWED	RENEW	SYSTEM
BASIC_APPLICATION_GROUP_CREATED	CREATE	GROUP
BASIC_APPLICATION_GROUP_MODIFIED	UPDATE	GROUP
MEMBER_ADDED_TO_BASIC_APPLICATION_GROUP	UPDATE	GROUP
MEMBER_REMOVED_FROM_BASIC_APPLICATION_GROUP	UPDATE	GROUP
NON-MEMBER_ADDED_TO_BASIC_APPLICATION_GROUP	UPDATE	GROUP
NON-MEMBER_REMOVED_FROM_BASIC_APPLICATION_GROUP	UPDATE	GROUP
BASIC_APPLICATION_GROUP_DELETED	DELETE	GROUP
LDAP_QUERY_GROUP_CREATED	CREATE	GROUP
COMPUTER_ACCOUNT_CREATED	CREATE	ACCOUNT
COMPUTER_ACCOUNT_MODIFIED	UPDATE	ACCOUNT

Table J–1 (Cont.) Windows Audit Events

Source Event	command_class	target_type
COMPUTER_ACCOUNT_DELETED	DELETE	ACCOUNT
SECURITY-DISABLED_LOCAL_GROUP_CREATED	CREATE	GROUP
SECURITY-DISABLED_LOCAL_GROUP_MODIFIED	UPDATE	GROUP
MEMBER_ADDED_TO_SECURITY-DISABLED_LOCAL_GROUP	UPDATE	GROUP
MEMBER_REMOVED_FROM_SECURITY-DISABLED_LOCAL_GROUP	UPDATE	GROUP
SECURITY-DISABLED_LOCAL_GROUP_DELETED	DELETE	GROUP
SECURITY-DISABLED_GLOBAL_GROUP_CREATED	CREATE	GROUP
SECURITY-DISABLED_GLOBAL_GROUP_MODIFIED	UPDATE	GROUP
MEMBER_ADDED_TO_SECURITY-DISABLED_GLOBAL_GROUP	UPDATE	GROUP
MEMBER_REMOVED_FROM_SECURITY-DISABLED_GLOBAL_GROUP	UPDATE	GROUP
SECURITY-DISABLED_GLOBAL_GROUP_DELETED	DELETE	GROUP
SECURITY-DISABLED_UNIVERSAL_GROUP_CREATED	CREATE	GROUP
SECURITY-DISABLED_UNIVERSAL_GROUP_MODIFIED	UPDATE	GROUP
MEMBER_ADDED_TO_SECURITY-DISABLED_UNIVERSAL_GROUP	UPDATE	GROUP
MEMBER_REMOVED_FROM_SECURITY-DISABLED_UNIVERSAL_GROUP	UPDATE	GROUP
SECURITY-DISABLED_UNIVERSAL_GROUP_DELETED	DELETE	GROUP
PASSWORD_POLICY_CHECKING_API_CALLED	CALL	POLICY
SECURITY-ENABLED_GLOBAL_GROUP_CREATED	CREATE	GROUP
MEMBER_ADDED_TO_SECURITY-ENABLED_GLOBAL_GROUP	UPDATE	GROUP
MEMBER_REMOVED_FROM_SECURITY-ENABLED_GLOBAL_GROUP	UPDATE	GROUP
SECURITY-ENABLED_GLOBAL_GROUP_DELETED	DELETE	GROUP
SECURITY-ENABLED_LOCAL_GROUP_CREATED	CREATE	GROUP
MEMBER_ADDED_TO_SECURITY-ENABLED_LOCAL_GROUP	UPDATE	GROUP
MEMBER_REMOVED_FROM_SECURITY-ENABLED_LOCAL_GROUP	UPDATE	GROUP
SECURITY-ENABLED_LOCAL_GROUP_DELETED	DELETE	GROUP
SECURITY-ENABLED_LOCAL_GROUP_MODIFIED	UPDATE	GROUP
SECURITY-ENABLED_GLOBAL_GROUP_MODIFIED	UPDATE	GROUP
SECURITY-ENABLED_UNIVERSAL_GROUP_CREATED	CREATE	GROUP
SECURITY-ENABLED_UNIVERSAL_GROUP_MODIFIED	UPDATE	GROUP
MEMBER_ADDED_TO_SECURITY-ENABLED_UNIVERSAL_GROUP	UPDATE	GROUP
MEMBER_REMOVED_FROM_SECURITY-ENABLED_UNIVERSAL_GROUP	UPDATE	GROUP
SECURITY-ENABLED_UNIVERSAL_GROUP_DELETED	DELETE	GROUP
CHANGED_TYPE_OR_SCOPE_OF_GROUP	UPDATE	GROUP
CREATED_USER_ACCOUNT	CREATE	ACCOUNT
ENABLED_USER_ACCOUNT	ENABLE	ACCOUNT
ATTEMPTED_TO_MODIFY_ACCOUNT_PASSWORD	UPDATE	ACCOUNT

Table J–1 (Cont.) Windows Audit Events

Source Event	command_ class	target_type
ATTEMPTED_TO_RESET_ACCOUNT_PASSWORD	RESET	ACCOUNT
DISABLED_USER_ACCOUNT	DISABLE	ACCOUNT
DELETED_USER_ACCOUNT	DELETE	ACCOUNT
MODIFIED_USER_ACCOUNT	UPDATE	ACCOUNT
LOCKED_OUT_USER_ACCOUNT	LOCK	ACCOUNT
SID_HISTORY_ADDED_TO_ACCOUNT	UPDATE	ACCOUNT
ATTEMPT_TO_ADD_SID_HISTORY_TO_ACCOUNT_FAILED	INSERT	ACCOUNT
UNLOCKED_USER_ACCOUNT	UNLOCK	ACCOUNT
ACL_SET_ON_ACCOUNT	SET	ACCOUNT
MODIFIED_ACCOUNT_NAME	UPDATE	ACCOUNT
MODIFIED_DIRECTORY_SERVICE_RESTORE_MODE_ADMIN_PASSWORD	UPDATE	SERVICE
BACKED_UP_CREDENTIAL_MANAGER_CREDENTIALS	BACKUP	MANAGER
RESTORED_CREDENTIAL_MANAGER_CREDENTIALS	RESTORE	MANAGER
CREATED_NEW_PROCESS	START	PROCESS
ASSIGNED_PRIMARY_TOKEN_TO_PROCESS	ASSIGN	PROCESS
EXITED_PROCESS	STOP	PROCESS
REMOTE_PROCEDURE_CALL_ATTEMPTED	REMOTE CALL	PROCEDURE
ACCOUNT_FAILED_TO_LOGON	LOGIN	ACCOUNT
LOGGED_OFF_ACCOUNT	LOGOUT	ACCOUNT
USER_INITIATED_LOGOFF	LOGOUT	ACCOUNT
ACCOUNT_LOGON_SUCCESSFUL	LOGIN	ACCOUNT
LOGON_ATTEMPTED_USING_EXPLICIT_CREDENTIAL	LOGIN	SYSTEM
NETWORK_POLICY_SERVER_GRANTED_USER_ACCESS	GRANT	USER
NETWORK_POLICY_SERVER_DENIED_USER_ACCESS	DENY	USER
NETWORK_POLICY_SERVER_DISCARDED_USER_REQUEST	DENY	USER
NETWORK_POLICY_SERVER_DISCARDED_USER_ACCOUNTING_REQUEST	DENY	USER
NETWORK_POLICY_SERVER_QUARANTINED_USER	QUARANTINE	USER
NETWORK_POLICY_SERVER_GRANTED_USER_ACCESS_WITH_PROBATION	GRANT	USER
NETWORK_POLICY_SERVER_GRANTED_FULL_ACCESS	GRANT	USER
NETWORK_POLICY_SERVER_LOCKED_USER_ACCOUNT	LOCK	ACCOUNT
NETWORK_POLICY_SERVER_UNLOCKED_USER_ACCOUNT	UNLOCK	ACCOUNT
REPLAY_ATTACK_DETECTED	GET	SYSTEM
SESSION_RECONNECTED_TO_WORKSTATION	CONNECT	WORKSTATION
SESSION_DISCONNECTED_FROM_WORKSTATION	DISCONNECT	WORKSTATION
LOCKED_WORKSTATION	LOCK	WORKSTATION
UNLOCKED_WORKSTATION	UNLOCK	WORKSTATION

Table J–1 (Cont.) Windows Audit Events

Source Event	command_class	target_type
INVOKED_SCREEN_SAVER	CALL	SCREEN SAVER
DISMISSED_SCREEN_SAVER	ABORT	SCREEN SAVER
REQUESTED_CREDENTIAL_DELEGATION_DISALLOWED_BY_POLICY	DENY	ACCOUNT
REQUEST_MADE_TO_AUTHENTICATE_WIRELESS_NETWORK	AUTHENTICATE	NETWORK
REQUEST_MADE_TO_AUTHENTICATE_WIRED_NETWORK	AUTHENTICATE	NETWORK
SPECIAL_GROUP_ASSIGNED_TO_LOGON	ASSIGN	ACCOUNT
CERTIFICATE_SERVICES_RECEIVED_RESUBMITTED_CERTIFICATE_REQUEST	RECEIVE	CERTIFICATE
CERTIFICATE_SERVICES_REVOKED_CERTIFICATE	REVOKE	CERTIFICATE
CERTIFICATE_SERVICES_RECEIVED_CERTIFICATE_REVOKATION_LIST_PUBLISH_REQUEST	RECEIVE	CRL
CERTIFICATE_SERVICES_PUBLISHED_CRL	PUBLISH	CRL
CERTIFICATE_REQUEST_EXTENSION_MODIFIED	UPDATE	CERTIFICATE
CERTIFICATE_REQUEST_ATTRIBUTES_MODIFIED	UPDATE	CERTIFICATE
CERTIFICATE_SERVICE_RECEIVED_SHUT_DOWN_REQUEST	RECEIVE	SERVICE
CERTIFICATE_SERVICE_BACKUP_STARTED	BACKUP	SERVICE
CERTIFICATE_SERVICE_BACKUP_COMPLETED	BACKUP	SERVICE
CERTIFICATE_SERVICE_RESTORE_STARTED	RESTORE	SERVICE
CERTIFICATE_SERVICE_RESTORE_COMPLETED	RESTORE	SERVICE
CERTIFICATE_SERVICE_STARTED	START	SERVICE
CERTIFICATE_SERVICE_STOPPED	STOP	SERVICE
CERTIFICATE_SERVICE_SECURITY_PERMISSIONS_MODIFIED	UPDATE	SERVICE
CERTIFICATE_SERVICE_RETRIEVED_ARCHIVED_KEY	RETRIEVE	SERVICE
CERTIFICATE_SERVICE_IMPORTED_CERTIFICATE_IN_ITS_DATABASE	IMPORT	SERVICE
AUDIT_FILTER_FOR_CERTIFICATE_SERVICE_CHANGED	UPDATE	SERVICE
CERTIFICATE_SERVICE_RECEIVED_CERTIFICATE_REQUEST	RECEIVE	SERVICE
CERTIFICATE_SERVICE_APPROVED_CERTIFICATE_REQUEST_AND_ISSUED_CERTIFICATE	GRANT	SERVICE
CERTIFICATE_SERVICE_DENIED_CERTIFICATE_REQUEST	DENY	SERVICE
CERTIFICATE_SERVICE_SET_CERTIFICATE_REQUEST_STATUS_TO_PENDING	SET	SERVICE
CERTIFICATE_MANAGER_SETTINGS_FOR_CERTIFICATE_SERVICE_MODIFIED	UPDATE	SERVICE
CERTIFICATE_SERVICE_CONFIGURATION_ENTRY_MODIFIED	UPDATE	SERVICE
CERTIFICATE_SERVICE_PROPERTY_MODIFIED	UPDATE	SERVICE
CERTIFICATE_SERVICE_ARCHIVED_KEY	ARCHIVE	SERVICE
CERTIFICATE_SERVICE_IMPORTED_AND_ARCHIVED_KEY	ARCHIVE	SERVICE
CERTIFICATE_SERVICE_PUBLISHED_CA_CERTIFICATE_TO_ACTIVE_DIRECTORY_DOMAIN_SERVICES	PUBLISH	SERVICE
ROWS_DELETED_FROM_CERTIFICATE_DATABASE	DELETE	DATABASE
ENABLED_ROLE_SEPERATION_ON_CERTIFICATION_AUTHORITY	ENABLE	ROLE

Table J–1 (Cont.) Windows Audit Events

Source Event	command_ class	target_type
CERTIFICATE_SERVICE_LOADED_TEMPLATE	LOAD	TEMPLATE
NETWORK_SHARE_OBJECT_ACCESSED	ACCESS	OBJECT
ATTEMPT_MADE_TO_CREATE_HARD_LINK	CREATE	FILE
TRANSACTION_STATE_CHANGED	UPDATE	SYSTEM
FILE_WAS_VIRTUALIZED	ASSIGN	FILE
SE_AUDITID_ETW_FIREWALL_APP_BLOCKED_FROM_LISTENING	BLOCK	APPLICATION
WINDOWS_FILTERING_PLATFORM_PERMITTED_APPLICATION_TO_LISTEN_ON_PORT	GRANT	APPLICATION
WINDOWS_FILTERING_PLATFORM_BLOCKED_APPLICATION_FROM_LISTENING_ON_PORT	BLOCK	APPLICATION
WINDOWS_FILTERING_PLATFORM_BLOCKED_CONNECTION	BLOCK	CONNECTION
WINDOWS_FILTERING_PLATFORM_PERMITTED_BIND_TO_LOCAL_PORT	GRANT	PORT
WINDOWS_FILTERING_PLATFORM_BLOCKED_BIND_TO_LOCAL_PORT	BLOCK	PORT
WINDOWS_FILTERING_PLATFORM_BLOCKED_PACKET	BLOCK	PACKET
RESTRICTIVE_WINDOWS_FILTERING_PLATFORM_BLOCKED_PACKET	BLOCK	PACKET
HANDLE_TO_OBJECT_REQUESTED	REQUEST	OBJECT
HANDLE_TO_OBJECT_CLOSED	CLOSE	OBJECT
ATTEMPT_MADE_TO_DUPLICATE_HANDLE_TO_OBJECT	ACCESS	OBJECT
APPLICATION_ATTEMPTED_TO_ACCESS_BLOCKED_ORDINAL	ACCESS	ORDINAL
INDIRECT_ACCESS_TO_OBJECT_REQUESTED	ACCESS	OBJECT
CREATED_SCHEDULED_TASK	CREATE	TASK
DELETED_SCHEDULED_TASK	DELETE	TASK
ENABLED_SCHEDULED_TASK	ENABLE	TASK
DISABLED_SCHEDULED_TASK	DISABLE	TASK
UPDATED_SCHEDULED_TASK	UPDATE	TASK
OBJECT_IN_COM+_CATALOG_MODIFIED	UPDATE	OBJECT
OBJECT_DELETED_FROM_COM+_CATALOG	DELETE	OBJECT
OBJECT_ADDED_TO_COM+_CATALOG	INSERT	OBJECT
MODIFIED_REGISTRY_VALUE	UPDATE	REGISTRY
VIRTUALIZED_REGISTRY_KEY	ASSIGN	REGISTRY
HANDLE_TO_OBJECT_REQUESTED_WITH_DELETE_INTENT	REQUEST	OBJECT
OBJECT_DELETED	DELETE	OBJECT
HANDLE_TO_OBJECT_REQUESTED	REQUEST	OBJECT
OBJECT_ACCESS_ATTEMPTED	ACCESS	OBJECT
AUDIT_POLICY_ON_OBJECT_CHANGED	AUDIT	POLICY
SYSTEM_AUDIT_POLICY_CHANGED	AUDIT	POLICY
ATTEMPT_MADE_TO_REGISTER_SECURITY_EVENT_SOURCE	REGISTER	LOG
ATTEMPT_MADE_TO_UNREGISTER_SECURITY_EVENT_SOURCE	UNREGISTER	LOG

Table J–1 (Cont.) Windows Audit Events

Source Event	command_class	target_type
CRASHONAUDITFAIL_VALUE_MODIFIED	UPDATE	CRASHONAUDITFAIL
MODIFIED_AUDITING_SETTINGS_ON_OBJECT	AUDIT	OBJECT
MODIFIED_SPECIAL_GROUPS_LOGON_TABLE	UPDATE	GROUP
MODIFIED_PER_USER_AUDIT_POLICY	AUDIT	POLICY
KERBEROS_POLICY_MODIFIED	UPDATE	POLICY
TRUSTED_DOMAIN_INFORMATION_MODIFIED	UPDATE	DOMAIN
GRANTED_SYSTEM_SECURITY_ACCESS_TO_ACCOUNT	GRANT	ACCOUNT
REMOVED_SYSTEM_SECURITY_ACCESS_FROM_ACCOUNT	DROP	ACCOUNT
MODIFIED_DOMAIN_POLICY	UPDATE	DOMAIN
NAMESPACE_COLLISION_DETECTED	GET	NAMESPACE
TRUSTED_FOREST_INFORMATION_ENTRY_ADDED	INSERT	INFORMATION
TRUSTED_FOREST_INFORMATION_ENTRY_REMOVED	DROP	INFORMATION
TRUSTED_FOREST_INFORMATION_ENTRY_MODIFIED	UPDATE	INFORMATION
USER_RIGHT_ASSIGNED	ASSIGN	USER
USER_RIGHT_REMOVED	DROP	USER
NEW_TRUST_CREATED_TO_DOMAIN	CREATE	DOMAIN
TRUST_TO_DOMAIN_REMOVED	DROP	DOMAIN
ENCRYPTED_DATA_RECOVERY_POLICY_MODIFIED	UPDATE	POLICY
SE_AUDITID_ETW_IPSEC_POLICY_START	START	SERVICE
SE_AUDITID_ETW_IPSEC_POLICY_DISABLED	DISABLE	SERVICE
APPLIED_PASTORE_ENGINE	APPLY	ENGINE
SE_AUDITID_ETW_IPSEC_POLICY_FAILURE	FAIL	SERVICE
SE_AUDITID_ETW_IPSEC_AUTHENTICATION_SET_ADD	INSERT	SETTING
SE_AUDITID_ETW_IPSEC_AUTHENTICATION_SET_CHANGE	UPDATE	SETTING
SE_AUDITID_ETW_IPSEC_AUTHENTICATION_SET_DELETE	DELETE	SETTING
SE_AUDITID_ETW_IPSEC_CONNECTION_SECURITY_ADD	INSERT	SETTING
SE_AUDITID_ETW_IPSEC_CONNECTION_SECURITY_CHANGE	UPDATE	SETTING
SE_AUDITID_ETW_IPSEC_CONNECTION_SECURITY_DELETE	DELETE	SETTING
SE_AUDITID_ETW_IPSEC_CRYPTO_SET_ADD	ADD	SETTINGS
SE_AUDITID_ETW_IPSEC_CRYPTO_SET_CHANGE	MODIFY	SETTINGS
SE_AUDITID_ETW_IPSEC_CRYPTO_SET_DELETE	DELETE	SETTINGS
WINDOWS_FILTERING_PLATFORM_CALLOUTS_MODIFIED	UPDATE	CALLOUT
WINDOWS_FILTERING_PLATFORM_PROVIDER_MODIFIED	UPDATE	PROVIDER
WINDOWS_FILTERING_PLATFORM_PROVIDER_CONTEXT_MODIFIED	UPDATE	CONTEXT
WINDOWS_FILTERING_PLATFORM_SUBLAYER_MODIFIED	UPDATE	SUBLAYER
SE_AUDITID_ETW_FIREWALL_STARTUP_STATE	START	FIREWALL

Table J–1 (Cont.) Windows Audit Events

Source Event	command_ class	target_type
SE_AUDITID_ETW_FIREWALL_STARTUP_STATE_RULE	READ	RULE
SE_AUDITID_ETW_FIREWALL_RULE_ADD	INSERT	RULE
SE_AUDITID_ETW_FIREWALL_RULE_CHANGE	UPDATE	RULE
SE_AUDITID_ETW_FIREWALL_RULE_DELETE	DELETE	RULE
SE_AUDITID_ETW_FIREWALL_RESTORE_DEFAULTS	RESTORE	FIREWALL
SE_AUDITID_ETW_FIREWALL_SETTING_CHANGE	UPDATE	FIREWALL
SE_AUDITID_ETW_FIREWALL_GROUP_POLICY_CHANGED	UPDATE	FIREWALL
SE_AUDITID_ETW_FIREWALL_PROFILE_CHANGE	UPDATE	PROFILE
WINDOWS_FILTERING_PLATFORM_CHANGED_FILTER	UPDATE	FILTER
ERROR_OCCURED_WHILE_PROCESSING_SECURITY_POLICY_IN_GROUP_POLICY_OBJECTS	GET	POLICY
OBJECT_PERMISSION_MODIFIED	UPDATE	OBJECT
SPECIAL_PRIVILEGES_ASSIGNED_TO_NEW_LOGON	ASSIGN	ACCOUNT
PRIVILEGED_SERVICE_CALLED	CALL	SERVICE
OPERATION_ATTEMPTED_ON_PRIVILEGED_OBJECT	EXECUTE	OBJECT
IPSEC_DROPPED_INBOUND_PACKET_THAT_FAILED_INTEGRITY_CHECK	DROP	PACKET
IPSEC_DROPPED_INBOUND_PACKET_THAT_FAILED_REPLAY_BACK	DROP	PACKET
IPSEC_DROPPED_INBOUND_PACKET_THAT_FAILED_REPLAY_BACK	DROP	PACKET
IPSEC_DROPPED_INSECURE_CLEAR_TEXT_PACKET	DROP	PACKET
IPSEC_RECEIVED_PACKET_FROM_REMOTE_COMPUTER_WITH_INCORRECT_SPI	RECEIVE	PACKET
SE_AUDITID_ETW_POLICYAGENT_IPSECSVC_SUCCESSFUL_START	START	SERVICE
SE_AUDITID_ETW_POLICYAGENT_IPSECSVC_SUCCESSFUL_SHUTDOWN	STOP	SERVICE
SE_AUDITID_ETW_POLICYAGENT_IPSECSVC_INTERFACE_LIST_INCOMPLETE	FAIL	SERVICE
SE_AUDITID_ETW_POLICYAGENT_IPSECSVC_RPC_INIT_FAILURE	FAIL	SERVICE
SE_AUDITID_ETW_POLICYAGENT_IPSECSVC_ERROR_SHUTDOWN	STOPE	SERVICE
SE_AUDITID_ETW_POLICYAGENT_IPSECSVC_FAILED_PNP_FILTER_PROCESSING	FAIL	SERVICE
SE_AUDITID_ETW_MPSFIREWALL_SERVICE_STARTUP	START	FIREWALL
SE_AUDITID_ETW_MPSFIREWALL_STOPPED	STOP	FIREWALL
SE_AUDITID_ETW_MPSFIREWALL_GET_POLICY_FAILURE	RETRIEVE	FIREWALL
SE_AUDITID_ETW_MPSFIREWALL_PARSE_POLICY_FAILURE	FAIL	FIREWALL
SE_AUDITID_ETW_MPSFIREWALL_INIT_DRIVER_FAILURE	FAIL	FIREWALL
SE_AUDITID_ETW_MPSFIREWALL_SERVICE_STARTUP_FAILURE	FAIL	FIREWALL
SE_AUDITID_ETW_FIREWALL_UPCALL_NOTIFICATION_ERROR	NOTIFY	FIREWALL
SE_AUDITID_ETW_MPSFIREWALL_DRIVER_STARTED	START	DRIVER
SE_AUDITID_ETW_MPSFIREWALL_DRIVER_STOPPED	STOP	DRIVER
SE_AUDITID_ETW_MPSFIREWALL_DRIVER_STARTUP_FAILURE	FAIL	DRIVER
SE_AUDITID_ETW_MPSFIREWALL_DRIVER_CRITICAL_ERROR	ABORT	DRIVER

Table J–1 (Cont.) Windows Audit Events

Source Event	command_class	target_type
KEY_FILE_OPERATION	READ	KEY
KEY_MIGRATION_OPERATION	MIGRATE	KEY
WINDOWS_STARTING_UP	STARTUP	OS
WINDOWS_SHUTTING_DOWN	SHUTDOWN	OS
SYSTEM_TIME_CHANGED	UPDATE	SYSTEM TIME
ADMINISTRATOR_RECOVERED_SYSTEM_FROM_CRASHONAUDITFAIL	RECOVER	SYSTEM
LOCAL_SECURITY_AUTHORITY_LOADED_AUTHENTICATION_PACKAGE	LOAD	AUTHORITY
TRUSTED_LOGON_PROCESS_REGISTERED_WITH_LOCAL_SECURITY_AUTHORITY	REGISTER	PROCESS
SECURITY_ACCOUNT_MANAGER_LOADED_NOTIFICATION_PACKAGE	LOAD	MANAGER
LOCAL_SECURITY_AUTHORITY_LOADED_SECURITY_PACKAGE	LOAD	AUTHORITY
SERVICE_INSTALLED_IN_SYSTEM	INSTALL	SERVICE
EXHAUSTED_INTERNAL_RESOURCES_ALLOCATED_FOR_QUEUING_OF_AUDIT_MESSAGES	EXCEED	MESSAGES
INVALID_USE_LOCAL_PROCEDURE_CALL_PORT_BY_AN_APPLICATION	INVALID	PORT
MONITORED_SECURITY_EVENT_PATTERN_OCCURRED	RECEIVE	PATTERN
RPC_DETECTED_INTEGRITY_VIOLATION_WHILE_DECRYPTING_INCOMING_MESSAGE	GET	MESSAGE
DETERMINED_INVALID_IMAGE_HASH_OF_FILE	CALCULATE	FILE
CRYPTROGRAPHIC_PRIMITIVE_OPERATION_FAILED	FAIL	OPERATION
VERIFICATION_OPERATION_FAILED	FAIL	OPERATION
CRYPTROGRAPHIC_OPERATION	EXECUTE	OPERATION
LDAP_QUERY_GROUP_MODIFIED	UPDATE	GROUP
LDAP_QUERY_GROUP_DELETED	DELETE	GROUP
CERTIFICATE_SERVICE_TEMPLATE_MODIFIED	UPDATE	TEMPLATE
CERTIFICATE_SERVICE_TEMPLATE_SECURITY_MODIFIED	UPDATE	TEMPLATE
OCSP_RESPONDER_SERVICE_STARTED	START	SERVICE
OCSP_RESPONDER_SERVICE_STOPPED	STOP	SERVICE
CONFIGURATION_ENTRY_CHANGED_IN_OCSP_RESPONDER_SERVICE	UPDATE	SERVICE
CONFIGURATION_ENTRY_CHANGED_IN_OCSP_RESPONDER_SERVICE	UPDATE	SERVICE
SECURITY_SETTING_MODIFIED_ON_OCSP_RESPONDER_SERVICE	UPDATE	SERVICE
REQUEST_SUBMITTED_TO_OCSP_RESPONDER_SERVICE	SUBMIT	SERVICE
OCSP_RESPODER_SERVICE_AUTOMATICALLY_MODIFIED_SIGNING_CERTIFICATE	UPDATE	CERTIFICATE
OCSP_REVOCATION_PROVIDER_UPDATED_REVOCATION_INFORMATION	UPDATE	INFORMATION
AUDIT_LOG_CLEARED	DELETE	AUDIT LOG
EVENT_LOGGING_SERVICE_HAS_SHUTDOWN	STOP	SERVICE
SECURITY_LOG_IS_FULL	EXCEED	AUDIT LOG
NETWORK_SHARE_OBJECT_ADDED	INSERT	OBJECT
NETWORK_SHARE_OBJECT_MODIFIED	UPDATE	OBJECT

Table J–1 (Cont.) Windows Audit Events

Source Event	command_ class	target_type
NETWORK_SHARE_OBJECT_DELETED	DELETE	OBJECT
MODIFIED_AUDITING_SETTINGS_ON_OBJECT	AUDIT	OBJECT
NETWORK_SHARE_OBJECT_CHECKED_TO_SEE_CLIENT_GRANTED_DESIRED_ACCESS	VALIDATE	OBJECT

K

Linux Operating System Audit Events

This appendix maps audit event names used in the Linux Operating System to their equivalent values in the **Additional Description**, **command_class** and **target_type** fields in the Oracle AVDF audit record. You can use the audit events mapped here to create custom audit reports using other Oracle Database reporting products or third-party tools. See also "Oracle Audit Vault and Database Firewall Database Schemas" on page A-1 for Oracle AVDF data warehouse details that may be useful in designing your own reports.

Table K–1 lists the Linux audit events and the equivalent Oracle AVDF events.

Table K–1 Linux Audit Events

Source Event	Additional Description	command_class	target_type
LOGIN	N/A	LOGON	SYSTEM
USER_AUTH	N/A	AUTHENTICATE	USER
USER_ACCT	N/A	AUTHORIZE	USER
CRED_ACQ	N/A	ACQUIRE	USER
CRED_DISP	N/A	RESET	USER
DAEMON_START	N/A	AUDIT	AUDITSERVICE
DAEMON_END	N/A	NOAUDIT	AUDITSERVICE
DAEMON_ABORT	N/A	TERMINATE	AUDITSERVICE
DAEMON_CONFIG	N/A	CONFIGURE	AUDITSERVICE
DAEMON_ROTATE	N/A	UPDATE	AUDITSERVICE
DAEMON_RESUME	N/A	RESUME	AUDITSERVICE
CONFIG_CHANGE	audit_enabled record field contains 1 or 2	AUDIT	AUDITSERVICE
CONFIG_CHANGE	audit_enabled record field contains 0	NOAUDIT	AUDITSERVICE
CONFIG_CHANGE	op record field contains add rule	AUDIT	AUDITSERVICE
CONFIG_CHANGE	op record field contains remove rule	NOAUDIT	AUDITSERVICE
CONFIG_CHANGE	audit_failure record field contains value 0	NOAUDIT	AUDITSERVICE
CONFIG_CHANGE	audit_failure record field contains value 1	NOAUDIT	AUDITSERVICE
CONFIG_CHANGE	audit_failure record field contains value 2	NOAUDIT	AUDITSERVICE
CONFIG_CHANGE	any other CONFIG_CHANGE cases not specified above	UPDATE	AUDITSERVICE
CRYPTO_SESSION	N/A	START	SESSION

Table K–1 (Cont.) Linux Audit Events

Source Event	Additional Description	command_class	target_type
AVC	N/A	ACCESS	PRIVILEGE
MAC_POLICY_LOAD	N/A	ENABLE	POLICY
MAC_STATUS	N/A	UPDATE	SYSTEM
MAC_CONFIG_CHANGE	N/A	MODIFY	RULE
MAC_UNLBL_ALLOW	N/A	UPDATE	MODULE
MAC_CIPSOV4_ADD	N/A	CREATE	MODULE
MAC_CIPSOV4_DEL	N/A	DELETE	USER
MAC_MAP_ADD	N/A	CREATE	MODULE
MAC_MAP_DEL	N/A	DELETE	MODULE
MAC_IPSEC_ADDSA	N/A	CREATE	MODULE
MAC_IPSEC_DELSA	N/A	DELETE	MODULE
MAC_IPSEC_ADDSPD	N/A	MODIFY	MODULE
MAC_IPSEC_DELSPD	N/A	DELETE	MODULE
ANOM_PROMISCUOUS	N/A	UPDATE	DEVICE
ANOM_ABEND	N/A	EXECUTE	MODULE
ANOM_LOGIN_ FAILURES	N/A	LOGIN	USER
ANOM_LOGIN_TIME	N/A	LOGIN	USER
ANOM_LOGIN_ SESSIONS	N/A	LOGIN	USER
ANOM_LOGIN_ LOCATION	N/A	LOGON	USER
RESP_ACCT_UNLOCK_ TIMED	N/A	ENABLE	USER
RESP_ACCT_LOCK	N/A	LOCK	USER
TTY	N/A	EXECUTE	KEYSTROKE
USER_AVC	N/A	ACCESS	PRIVILEGE
USER_ROLE_CHANGE	op record field is not present	MODIFY	USER
USER_ROLE_CHANGE	op record field contains add SELinux user record	ADD	USER
USER_ROLE_CHANGE	op record field contains delete SELinux user record	DELETE	USER
USER_ROLE_CHANGE	any other USER_ROLE_CHANGE cases not specified above	MODIFY	USER
LABEL_OVERRIDE	N/A	UPDATE	OBJECT
LABEL_LEVEL_CHANGE	N/A	UPDATE	OBJECT
USER_LABELED_ EXPORT	N/A	EXPORT	OBJECT
USER_UNLABELED_ EXPORT	N/A	EXPORT	OBJECT
USER_START	N/A	START	USER

Table K–1 (Cont.) Linux Audit Events

Source Event	Additional Description	command_class	target_type
USER_END	N/A	END	USER
CRED_REFR	N/A	REFRESH	USER
USER_LOGIN	N/A	LOGIN	ACCOUNT
USER_LOGOUT	N/A	LOGOUT	ACCOUNT
USER_ERR	N/A	RAISE	USER
USYS_CONFIG	N/A	UPDATE	USER
USER_CMD	N/A	EXECUTE	PROGRAM
FS_RELABEL	N/A	MODIFY	SYSTEM
USER_CHAUTHTOK	op record field contains value change password	UPDATE	USER
USER_CHAUTHTOK	op record field contains value changing password	UPDATE	USER
USER_CHAUTHTOK	op record field contains value change expired password	UPDATE	USER
USER_CHAUTHTOK	op record field contains value change age	UPDATE	USER
USER_CHAUTHTOK	op record field contains value change max age	UPDATE	USER
USER_CHAUTHTOK	op record field contains value change min age	UPDATE	USER
USER_CHAUTHTOK	op record field contains value change passwd warning	UPDATE	USER
USER_CHAUTHTOK	op record field contains value change inactive days	UPDATE	USER
USER_CHAUTHTOK	op record field contains value change passwd expiration	UPDATE	USER
USER_CHAUTHTOK	op record field contains value change last change date	UPDATE	USER
USER_CHAUTHTOK	op record field contains value change all aging information	UPDATE	USER
USER_CHAUTHTOK	op record field contains value password attribute change	UPDATE	USER
USER_CHAUTHTOK	op record field contains value password aging data updated	UPDATE	USER
USER_CHAUTHTOK	op record field contains value display aging info	READ	USER
USER_CHAUTHTOK	op record field contains value password status display	READ	USER
USER_CHAUTHTOK	op record field contains value password status displayed for user	READ	USER
USER_CHAUTHTOK	op record field contains value adding to group	CREATE	USER
USER_CHAUTHTOK	op record field contains value adding group member	CREATE	USER

Table K–1 (Cont.) Linux Audit Events

Source Event	Additional Description	command_class	target_type
USER_CHAUTHTOK	op record field contains value adding user to group	CREATE	USER
USER_CHAUTHTOK	op record field contains value adding user to shadow group	CREATE	USER
USER_CHAUTHTOK	op record field contains value changing primary group	UPDATE	USER
USER_CHAUTHTOK	op record field contains value changing group member	UPDATE	USER
USER_CHAUTHTOK	op record field contains value changing admin name in shadow group	UPDATE	USER
USER_CHAUTHTOK	op record field contains value changing member in shadow group	UPDATE	USER
USER_CHAUTHTOK	op record field contains value deleting group password	DELETE	USER
USER_CHAUTHTOK	op record field contains value deleting member	DELETE	USER
USER_CHAUTHTOK	op record field contains value deleting user from group	DELETE	USER
USER_CHAUTHTOK	op record field contains value deleting user from shadow group	DELETE	USER
USER_CHAUTHTOK	op record field contains value removing group member	DELETE	USER
USER_CHAUTHTOK	op record field contains value removing user from shadow group	DELETE	USER
USER_CHAUTHTOK	op record field contains value user lookup	UPDATE	USER
USER_CHAUTHTOK	op record field contains value adding group	CREATE	USER
USER_CHAUTHTOK	op record field contains value deleting group	DELETE	USER
USER_CHAUTHTOK	op record field contains value adding user	CREATE	USER
USER_CHAUTHTOK	op record field contains value adding home directory	CREATE	USER
USER_CHAUTHTOK	op record field contains value deleting user entries	DELETE	USER
USER_CHAUTHTOK	op record field contains value deleting user not found	DELETE	USER
USER_CHAUTHTOK	op record field contains value deleting user	DELETE	USER
USER_CHAUTHTOK	op record field contains value deleting user logged in	DELETE	USER
USER_CHAUTHTOK	op record field contains value deleting mail file	DELETE	USER
USER_CHAUTHTOK	op record field contains value deleting home directory	DELETE	USER
USER_CHAUTHTOK	op record field contains value lock password	LOCK	USER
USER_CHAUTHTOK	op record field contains value delete password	DELETE	USER

Table K–1 (Cont.) Linux Audit Events

Source Event	Additional Description	command_class	target_type
USER_CHAUTHTOK	op record field contains value updating password	UPDATE	USER
USER_CHAUTHTOK	op record field contains value unlock password	UNLOCK	USER
USER_CHAUTHTOK	op record field contains value changing name	RENAME	USER
USER_CHAUTHTOK	op record field contains value changing uid	UPDATE	USER
USER_CHAUTHTOK	op record field contains value changing home directory	UPDATE	USER
USER_CHAUTHTOK	op record field contains value moving home directory	MOVE	USER
USER_CHAUTHTOK	op record field contains value changing mail file name	RENAME	USER
USER_CHAUTHTOK	op record field contains value changing mail file owner	UPDATE	USER
USER_CHAUTHTOK	N/A	UPDATE	USER
USER_TTY	N/A	EXECUTE	KEYSTROKE
ADD_GROUP	N/A	ADD	GROUP
ADD_USER	N/A	CREATE	USER
DEL_USER	N/A	DELETE	USER
SYSCALL	N/A	EXECUTE	SYSCALL
SYSCALL	SYSCALL record field contains value 0	READ	FILE
SYSCALL	SYSCALL record field contains value 1	WRITE	FILE
SYSCALL	SYSCALL record field contains value 2	OPEN	FILE
SYSCALL	SYSCALL record field contains value 3	CLOSE	FILE
SYSCALL	SYSCALL record field contains value 4	GET	FILE
SYSCALL	SYSCALL record field contains value 5	GET	FILE
SYSCALL	SYSCALL record field contains value 6	GET	FILE
SYSCALL	SYSCALL record field contains value 7	GET	FILE
SYSCALL	SYSCALL record field contains value 8	GET	FILE OFFSET
SYSCALL	SYSCALL record field contains value 9	SET	PAGE
SYSCALL	SYSCALL record field contains value 10	EXECUTE	MEMORY
SYSCALL	SYSCALL record field contains value 11	RESET	PAGE
SYSCALL	SYSCALL record field contains value 12	UPDATE	SPACE
SYSCALL	SYSCALL record field contains value 13	UPDATE	ACTION
SYSCALL	SYSCALL record field contains value 14	ACCESS	SIGNAL MASK
SYSCALL	SYSCALL record field contains value 15	UNDO	PROCESS
SYSCALL	SYSCALL record field contains value 16	CONTROL	DEVICE
SYSCALL	SYSCALL record field contains value 17	READ	FILE
SYSCALL	SYSCALL record field contains value 18	INSERT	FILE

Table K–1 (Cont.) Linux Audit Events

Source Event	Additional Description	command_class	target_type
SYSCALL	SYSCALL record field contains value 19	READ	FILE
SYSCALL	SYSCALL record field contains value 20	INSERT	FILE
SYSCALL	SYSCALL record field contains value 21	VALIDATE	PERMISSION
SYSCALL	SYSCALL record field contains value 22	CREATE	CHANNEL
SYSCALL	SYSCALL record field contains value 23	EXECUTE	FILE
SYSCALL	SYSCALL record field contains value 24	ACQUIRE	CPU
SYSCALL	SYSCALL record field contains value 25	RESET	MEMORY ADDRESS
SYSCALL	SYSCALL record field contains value 26	SYNCHRONIZE	FILE
SYSCALL	SYSCALL record field contains value 27	GET	PAGE
SYSCALL	SYSCALL record field contains value 28	EXECUTE	MEMORY
SYSCALL	SYSCALL record field contains value 29	ASSIGN	SEGMENT
SYSCALL	SYSCALL record field contains value 30	EXECUTE	MEMORY
SYSCALL	SYSCALL record field contains value 31	CONTROL	MEMORY
SYSCALL	SYSCALL record field contains value 32	COPY	FILE
SYSCALL	SYSCALL record field contains value 33	COPY	FILE
SYSCALL	SYSCALL record field contains value 34	WAIT	SIGNAL
SYSCALL	SYSCALL record field contains value 35	SUSPEND	THREAD
SYSCALL	SYSCALL record field contains value 36	GET	TIMER
SYSCALL	SYSCALL record field contains value 37	SET	ALARM
SYSCALL	SYSCALL record field contains value 38	SET	TIMER
SYSCALL	SYSCALL record field contains value 39	GET	PROCESS
SYSCALL	SYSCALL record field contains value 40	SEND	FILE
SYSCALL	SYSCALL record field contains value 41	CREATE	COMMUNICATION ENDPOINT
SYSCALL	SYSCALL record field contains value 42	CONNECT	SOCKET
SYSCALL	SYSCALL record field contains value 43	ACQUIRE	SOCKET CONNECTION
SYSCALL	SYSCALL record field contains value 44	SEND	MESSAGE
SYSCALL	SYSCALL record field contains value 45	RECEIVE	MESSAGE
SYSCALL	SYSCALL record field contains value 46	SEND	MESSAGE
SYSCALL	SYSCALL record field contains value 47	RECEIVE	MESSAGE
SYSCALL	SYSCALL record field contains value 48	STOP	CONNECTION
SYSCALL	SYSCALL record field contains value 49	BIND	NAME
SYSCALL	SYSCALL record field contains value 50	EXECUTE	CONNECTION
SYSCALL	SYSCALL record field contains value 51	GET	SOCKET
SYSCALL	SYSCALL record field contains value 52	GET	SOCKET
SYSCALL	SYSCALL record field contains value 53	CREATE	SOCKET
SYSCALL	SYSCALL record field contains value 54	SET	SOCKET

Table K–1 (Cont.) Linux Audit Events

Source Event	Additional Description	command_class	target_type
SYSCALL	SYSCALL record field contains value 55	GET	SOCKET
SYSCALL	SYSCALL record field contains value 56	COPY	PROCESS
SYSCALL	SYSCALL record field contains value 57	EXECUTE	PROCESS
SYSCALL	SYSCALL record field contains value 58	EXECUTE	PROCESS
SYSCALL	SYSCALL record field contains value 59	EXECUTE	PROCESS
SYSCALL	SYSCALL record field contains value 60	STOP	PROCESS
SYSCALL	SYSCALL record field contains value 61	WAIT	PROCESS
SYSCALL	SYSCALL record field contains value 62	SEND	SIGNAL
SYSCALL	SYSCALL record field contains value 63	GET	NAME
SYSCALL	SYSCALL record field contains value 64	GET	SEMAPHORE
SYSCALL	SYSCALL record field contains value 65	EXECUTE	SEMAPHORE
SYSCALL	SYSCALL record field contains value 66	CONTROL	SEMAPHORE
SYSCALL	SYSCALL record field contains value 67	EXECUTE	MEMORY
SYSCALL	SYSCALL record field contains value 68	GET	QUEUE ID
SYSCALL	SYSCALL record field contains value 69	SEND	MESSAGE
SYSCALL	SYSCALL record field contains value 70	RECEIVE	MESSAGE
SYSCALL	SYSCALL record field contains value 71	CONTROL	MESSAGE
SYSCALL	SYSCALL record field contains value 72	UPDATE	FILE
SYSCALL	SYSCALL record field contains value 73	LOCK	FILE
SYSCALL	SYSCALL record field contains value 74	SYNCHRONIZE	FILE
SYSCALL	SYSCALL record field contains value 75	SYNCHRONIZE	FILE
SYSCALL	SYSCALL record field contains value 76	TRUNCATE	FILE
SYSCALL	SYSCALL record field contains value 77	TRUNCATE	FILE
SYSCALL	SYSCALL record field contains value 78	GET	ENTRIES
SYSCALL	SYSCALL record field contains value 79	GET	DIRECTORY
SYSCALL	SYSCALL record field contains value 80	UPDATE	DIRECTORY
SYSCALL	SYSCALL record field contains value 81	UPDATE	DIRECTORY
SYSCALL	SYSCALL record field contains value 82	UPDATE	FILE
SYSCALL	SYSCALL record field contains value 83	CREATE	DIRECTORY
SYSCALL	SYSCALL record field contains value 84	DELETE	DIRECTORY
SYSCALL	SYSCALL record field contains value 85	CREATE	FILE OR DEVICE
SYSCALL	SYSCALL record field contains value 86	CONNECT	FILE
SYSCALL	SYSCALL record field contains value 87	DISCONNECT	FILE
SYSCALL	SYSCALL record field contains value 88	CONNECT	FILE
SYSCALL	SYSCALL record field contains value 89	READ	VALUE
SYSCALL	SYSCALL record field contains value 90	UPDATE	FILE
SYSCALL	SYSCALL record field contains value 91	UPDATE	FILE

Table K–1 (Cont.) Linux Audit Events

Source Event	Additional Description	command_class	target_type
SYSCALL	SYSCALL record field contains value 92	UPDATE	OWNERSHIP
SYSCALL	SYSCALL record field contains value 93	UPDATE	OWNERSHIP
SYSCALL	SYSCALL record field contains value 94	UPDATE	OWNERSHIP
SYSCALL	SYSCALL record field contains value 95	SET	MASK
SYSCALL	SYSCALL record field contains value 96	GET	TIME
SYSCALL	SYSCALL record field contains value 97	GET	LIMIT
SYSCALL	SYSCALL record field contains value 98	GET	USAGE
SYSCALL	SYSCALL record field contains value 99	GET	INFORMATION
SYSCALL	SYSCALL record field contains value 100	GET	TIME
SYSCALL	SYSCALL record field contains value 101	SEARCH	PROCESS
SYSCALL	SYSCALL record field contains value 102	GET	USER
SYSCALL	SYSCALL record field contains value 103	READ	LOG
SYSCALL	SYSCALL record field contains value 104	GET	GROUP
SYSCALL	SYSCALL record field contains value 105	SET	USER
SYSCALL	SYSCALL record field contains value 106	GET	GROUP
SYSCALL	SYSCALL record field contains value 107	GET	USER
SYSCALL	SYSCALL record field contains value 108	GET	GROUP
SYSCALL	SYSCALL record field contains value 109	SET	GROUP
SYSCALL	SYSCALL record field contains value 110	GET	PROCESS
SYSCALL	SYSCALL record field contains value 111	GET	PROCESS GROUP
SYSCALL	SYSCALL record field contains value 112	SET	PROCESS GROUP
SYSCALL	SYSCALL record field contains value 113	SET	USER
SYSCALL	SYSCALL record field contains value 114	SET	GROUP
SYSCALL	SYSCALL record field contains value 115	GET	GROUP
SYSCALL	SYSCALL record field contains value 116	SET	GROUP
SYSCALL	SYSCALL record field contains value 117	SET	USER
SYSCALL	SYSCALL record field contains value 118	GET	USER
SYSCALL	SYSCALL record field contains value 119	SET	GROUP
SYSCALL	SYSCALL record field contains value 120	GET	GROUP
SYSCALL	SYSCALL record field contains value 121	GET	PROCESS GROUP
SYSCALL	SYSCALL record field contains value 122	SET	USER IDENTITY
SYSCALL	SYSCALL record field contains value 123	SET	GROUP IDENTITY
SYSCALL	SYSCALL record field contains value 124	GET	SESSION
SYSCALL	SYSCALL record field contains value 125	GET	CAPABILITIES
SYSCALL	SYSCALL record field contains value 126	SET	CAPABILITIES
SYSCALL	SYSCALL record field contains value 127	SEARCH	SIGNAL
SYSCALL	SYSCALL record field contains value 128	WAIT	SIGNAL

Table K–1 (Cont.) Linux Audit Events

Source Event	Additional Description	command_class	target_type
SYSCALL	SYSCALL record field contains value 129	QUEUE	SIGNAL
SYSCALL	SYSCALL record field contains value 130	WAIT	SIGNAL
SYSCALL	SYSCALL record field contains value 131	SET	CONTEXT
SYSCALL	SYSCALL record field contains value 132	UPDATE	TIME
SYSCALL	SYSCALL record field contains value 133	CREATE	FILE
SYSCALL	SYSCALL record field contains value 134	EXECUTE	SYSTEM CALLS
SYSCALL	SYSCALL record field contains value 135	SET	DOMAIN
SYSCALL	SYSCALL record field contains value 136	GET	STATISTICS
SYSCALL	SYSCALL record field contains value 137	GET	STATISTICS
SYSCALL	SYSCALL record field contains value 138	GET	STATISTICS
SYSCALL	SYSCALL record field contains value 139	GET	INFORMATION
SYSCALL	SYSCALL record field contains value 140	GET	PRIORITY
SYSCALL	SYSCALL record field contains value 141	SET	PRIORITY
SYSCALL	SYSCALL record field contains value 142	SET	PARAMETERS
SYSCALL	SYSCALL record field contains value 143	GET	PARAMETERS
SYSCALL	SYSCALL record field contains value 144	SET	POLICY OR PARAMETERS
SYSCALL	SYSCALL record field contains value 145	GET	POLICY OR PARAMETERS
SYSCALL	SYSCALL record field contains value 146	GET	PRIORITY
SYSCALL	SYSCALL record field contains value 147	GET	PRIORITY
SYSCALL	SYSCALL record field contains value 148	GET	INTERVAL
SYSCALL	SYSCALL record field contains value 149	LOCK	MEMORY
SYSCALL	SYSCALL record field contains value 150	UNLOCK	MEMORY
SYSCALL	SYSCALL record field contains value 151	LOCK	MEMORY
SYSCALL	SYSCALL record field contains value 152	UNLOCK	MEMORY
SYSCALL	SYSCALL record field contains value 153	WAIT	TERMINAL
SYSCALL	SYSCALL record field contains value 154	UPDATE	TABLE
SYSCALL	SYSCALL record field contains value 155	UPDATE	FILE
SYSCALL	SYSCALL record field contains value 156	UPDATE	PARAMETERS
SYSCALL	SYSCALL record field contains value 157	EXECUTE	PROCESS
SYSCALL	SYSCALL record field contains value 158	SET	STATE
SYSCALL	SYSCALL record field contains value 159	SET	STATE
SYSCALL	SYSCALL record field contains value 160	SET	RESOURCE LIMIT
SYSCALL	SYSCALL record field contains value 161	UPDATE	DIRECTORY
SYSCALL	SYSCALL record field contains value 162	COMMIT	CACHE
SYSCALL	SYSCALL record field contains value 163	UPDATE	ACCOUNTING
SYSCALL	SYSCALL record field contains value 164	SET	TIME

Table K–1 (Cont.) Linux Audit Events

Source Event	Additional Description	command_class	target_type
SYSCALL	SYSCALL record field contains value 165	MOUNT	FILE
SYSCALL	SYSCALL record field contains value 166	UNMOUNT	FILE
SYSCALL	SYSCALL record field contains value 167	START	FILE
SYSCALL	SYSCALL record field contains value 168	STOP	FILE
SYSCALL	SYSCALL record field contains value 169	START	SYSTEM
SYSCALL	SYSCALL record field contains value 170	SET	HOSTNAME
SYSCALL	SYSCALL record field contains value 171	SET	DOMAINNAME
SYSCALL	SYSCALL record field contains value 172	UPDATE	IOPL
SYSCALL	SYSCALL record field contains value 173	UPDATE	PERMISSION
SYSCALL	SYSCALL record field contains value 174	CREATE	MODULE
SYSCALL	SYSCALL record field contains value 175	INITIALIZE	MODULE
SYSCALL	SYSCALL record field contains value 176	DELETE	MODULE
SYSCALL	SYSCALL record field contains value 177	GET	KERNEL
SYSCALL	SYSCALL record field contains value 178	QUERY	KERNEL
SYSCALL	SYSCALL record field contains value 179	EXECUTE	QUOTAS
SYSCALL	SYSCALL record field contains value 180	EXECUTE	KERNEL
SYSCALL	SYSCALL record field contains value 186	GET	THREAD
SYSCALL	SYSCALL record field contains value 187	LOAD	CACHE
SYSCALL	SYSCALL record field contains value 188	SET	ATTRIBUTE
SYSCALL	SYSCALL record field contains value 189	SET	ATTRIBUTE
SYSCALL	SYSCALL record field contains value 190	SET	ATTRIBUTE
SYSCALL	SYSCALL record field contains value 191	GET	ATTRIBUTE
SYSCALL	SYSCALL record field contains value 192	GET	ATTRIBUTE
SYSCALL	SYSCALL record field contains value 193	GET	ATTRIBUTE
SYSCALL	SYSCALL record field contains value 194	READ	ATTRIBUTE
SYSCALL	SYSCALL record field contains value 195	READ	ATTRIBUTE
SYSCALL	SYSCALL record field contains value 196	READ	ATTRIBUTE
SYSCALL	SYSCALL record field contains value 197	DELETE	ATTRIBUTE
SYSCALL	SYSCALL record field contains value 198	DELET	ATTRIBUTE
SYSCALL	SYSCALL record field contains value 199	DELETE	ATTRIBUTE
SYSCALL	SYSCALL record field contains value 200	SEND	SIGNAL
SYSCALL	SYSCALL record field contains value 201	GET	TIME
SYSCALL	SYSCALL record field contains value 202	WAIT	ADDRESS
SYSCALL	SYSCALL record field contains value 203	SET	MASK
SYSCALL	SYSCALL record field contains value 204	GET	MASK
SYSCALL	SYSCALL record field contains value 205	SET	STORAGE
SYSCALL	SYSCALL record field contains value 206	CREATE	CONTEXT

Table K–1 (Cont.) Linux Audit Events

Source Event	Additional Description	command_class	target_type
SYSCALL	SYSCALL record field contains value 207	DELETE	CONTEXT
SYSCALL	SYSCALL record field contains value 208	READ	EVENTS
SYSCALL	SYSCALL record field contains value 209	SUBMIT	BLOCK
SYSCALL	SYSCALL record field contains value 210	CANCEL	OPERATION
SYSCALL	SYSCALL record field contains value 211	GET	STORAGE
SYSCALL	SYSCALL record field contains value 212	RESUME	PATH
SYSCALL	SYSCALL record field contains value 213	OPEN	FILE
SYSCALL	SYSCALL record field contains value 215	WAIT	FILE
SYSCALL	SYSCALL record field contains value 216	CREATE	MAPPING
SYSCALL	SYSCALL record field contains value 217	GET	DIRECTORY
SYSCALL	SYSCALL record field contains value 218	SET	POINTER
SYSCALL	SYSCALL record field contains value 219	START	SYSCALL
SYSCALL	SYSCALL record field contains value 220	EXECUTE	SEMAPHORE
SYSCALL	SYSCALL record field contains value 221	SUBSCRIBE	PATTERN
SYSCALL	SYSCALL record field contains value 222	CREATE	TIMER
SYSCALL	SYSCALL record field contains value 223	EXECUTE	TIMER
SYSCALL	SYSCALL record field contains value 224	EXECUTE	TIMER
SYSCALL	SYSCALL record field contains value 225	GET	TIMER
SYSCALL	SYSCALL record field contains value 226	DELETE	TIMER
SYSCALL	SYSCALL record field contains value 227	SET	CLOCK
SYSCALL	SYSCALL record field contains value 228	GET	CLOCK
SYSCALL	SYSCALL record field contains value 229	FIND	CLOCK
SYSCALL	SYSCALL record field contains value 230	WAIT	CLOCK
SYSCALL	SYSCALL record field contains value 231	EXIT	THREAD
SYSCALL	SYSCALL record field contains value 232	WAIT	EVENT
SYSCALL	SYSCALL record field contains value 234	SEND	SIGNAL
SYSCALL	SYSCALL record field contains value 235	UPDATE	TIME
SYSCALL	SYSCALL record field contains value 237	EXECUTE	SET
SYSCALL	SYSCALL record field contains value 238	EXECUTE	SET
SYSCALL	SYSCALL record field contains value 239	SET	SET
SYSCALL	SYSCALL record field contains value 240	OPEN	QUEUE
SYSCALL	SYSCALL record field contains value 241	DISCONNECT	QUEUE
SYSCALL	SYSCALL record field contains value 242	SEND	MESSAGE
SYSCALL	SYSCALL record field contains value 243	RECEIVE	MESSAGE
SYSCALL	SYSCALL record field contains value 244	REGISTER	NOTIFICATION
SYSCALL	SYSCALL record field contains value 245	GET	ATTRIBUTE
SYSCALL	SYSCALL record field contains value 246	LOAD	KERNEL

Table K–1 (Cont.) Linux Audit Events

Source Event	Additional Description	command_class	target_type
SYSCALL	SYSCALL record field contains value 247	WAIT	PROCESS
SYSCALL	SYSCALL record field contains value 248	CREATE	KEY
SYSCALL	SYSCALL record field contains value 249	REQUEST	KEY
SYSCALL	SYSCALL record field contains value 250	EXECUTE	KERNEL
SYSCALL	SYSCALL record field contains value 251	SET	PRIORITY
SYSCALL	SYSCALL record field contains value 252	GET	PRIORITY
SYSCALL	SYSCALL record field contains value 253	INITIALIZE	INSTANCE
SYSCALL	SYSCALL record field contains value 254	CREATE	INSTANCE
SYSCALL	SYSCALL record field contains value 255	DELETE	INSTANCE
SYSCALL	SYSCALL record field contains value 256	MOVE	PAGE
SYSCALL	SYSCALL record field contains value 257	OPEN	FILE
SYSCALL	SYSCALL record field contains value 258	CREATE	DIRECTORY
SYSCALL	SYSCALL record field contains value 259	CREATE	FILE
SYSCALL	SYSCALL record field contains value 260	UPDATE	FILE OR DIRECTORY
SYSCALL	SYSCALL record field contains value 261	UPDATE	TIMESTAMP
SYSCALL	SYSCALL record field contains value 262	GET	STATUS
SYSCALL	SYSCALL record field contains value 263	REMOVE	FILE
SYSCALL	SYSCALL record field contains value 264	RENAME	FILE
SYSCALL	SYSCALL record field contains value 265	CREATE	LINK
SYSCALL	SYSCALL record field contains value 266	CREATE	LINK
SYSCALL	SYSCALL record field contains value 267	READ	LINK
SYSCALL	SYSCALL record field contains value 268	UPDATE	FILE
SYSCALL	SYSCALL record field contains value 269	VALIDATE	FILE
SYSCALL	SYSCALL record field contains value 270	EXECUTE	FILE
SYSCALL	SYSCALL record field contains value 271	WAIT	EVENT
SYSCALL	SYSCALL record field contains value 272	DISASSOCIATE	CONTEXT
SYSCALL	SYSCALL record field contains value 273	SET	LIST
SYSCALL	SYSCALL record field contains value 274	GET	LIST
SYSCALL	SYSCALL record field contains value 275	EXECUTE	DATA
SYSCALL	SYSCALL record field contains value 276	COPY	CONTENT
SYSCALL	SYSCALL record field contains value 277	SYNCHRONIZE	SEGMENT
SYSCALL	SYSCALL record field contains value 278	EXECUTE	PAGE
SYSCALL	SYSCALL record field contains value 279	MOVE	PAGE
SYSCALL	SYSCALL record field contains value 280	UPDATE	TIMESTAMP
SYSCALL	SYSCALL record field contains value 281	WAIT	EVENT
SYSCALL	SYSCALL record field contains value 282	CREATE	FILE
SYSCALL	SYSCALL record field contains value 283	EXECUTE	TIMER

Table K–1 (Cont.) Linux Audit Events

Source Event	Additional Description	command_class	target_type
SYSCALL	SYSCALL record field contains value 284	CREATE	FILE
SYSCALL	SYSCALL record field contains value 285	EXECUTE	SPACE
SYSCALL	SYSCALL record field contains value 286	CREATE	TIMER
SYSCALL	SYSCALL record field contains value 287	GET	TIMER
SYSCALL	SYSCALL record field contains value 288	ACQUIRE	CONNECTION
SYSCALL	SYSCALL record field contains value 289	CREATE	FILE
SYSCALL	SYSCALL record field contains value 290	CREATE	FILE
SYSCALL	SYSCALL record field contains value 291	OPEN	FILE
SYSCALL	SYSCALL record field contains value 292	COPY	FILE
SYSCALL	SYSCALL record field contains value 293	CREATE	PIPE
SYSCALL	SYSCALL record field contains value 294	INITIALIZE	INSTANCE
SYSCALL	SYSCALL record field contains value 295	READ	DATA
SYSCALL	SYSCALL record field contains value 296	WRITE	DATA
SYSCALL	SYSCALL record field contains value 297	SUBSCRIBE	DATA
SYSCALL	SYSCALL record field contains value 298	CREATE	FILE
SELINUX_ERR	N/A	RAISE	SYSTEM
SYSTEM_SHUTDOWN	N/A	SHUTDOWN	OS
ROLE_REMOVE	N/A	DELETE	ROLE
ROLE_ASSIGN	N/A	ASSIGN	ROLE
SYSTEM_RUNLEVEL	N/A	STOP	SYSTEM
NETFILTER_CFG	N/A	CONFIGURE	SOCKET
DEL_GROUP	N/A	DELETE	GROUP
CRYPTO_KEY_USER	N/A	DISCONNECT	USER SESSION

L

Oracle ACFS Audit Events

This appendix maps audit event names used in the Oracle ACFS to their equivalent values in the **Source Event**, **Command Class**, **Target Object**, **Associate Object** fields and the **Status** of the event occurred on target object in the Oracle AVDF audit record.

Target Object can be either a **Security Object**, for example: Realm, Rules, Rulesets, and so on, or, a **File System Object** like File or Dir.

Event or **Command Class** can be of the following types.

- For security objects `CREATE`, `MODIFY`, `DELETE` and so on. For example, if a realm is getting created, realm is target object and `ACFS_SEC_REALM_CREATE` is the event which is being mapped to the command class `CREATE` (selected from a set given by Oracle AVDF).
- For filesystem object `READ`, `WRITE`, `OPEN`, `DELETE` and so on. For example, if a file is being read, file is target object, and `ACFS_EVENT_READ_OP` is event which is being mapped to command class `READ` (selected from set given by Oracle AVDF).

Associate Objects are the objects which are associated while an event is performed on a Target Object. For example, in Security commands where we add files to the realm as follows: Target object- realm, Event- `ACFS_SEC_REALM_ADD` (`MODIFY`), Associate object- file. Another example would be where a file is being read by a user: Target object- file, Event- `ACFS_AUDIT_READ_OP` (`READ`), Associate objects- realms.

The **Status** column specifies whether the command class executed on the target object succeeded or not.

See also "Oracle Audit Vault and Database Firewall Database Schemas" on page A-1 for Oracle AVDF data warehouse details that may be useful in designing your own reports.

Table L–1 lists the Oracle ACFS Security Objects audit events and the equivalent Oracle AVDF events.

Table L–1 ACFS Security Objects Audit Events

Source Event	Command Class	Target Object	Associate Objects	Status
`ACFS_SEC_PREPARE`	`ENABLE`	MountPoint	Security	`SUCCESS`
`ACFS_SEC_REALM_CREATE`	`CREATE`	Realm name	None	`SUCCESS`
`ACFS_SEC_REALM_DESTROY`	`DELETE`	Realm name	None	`SUCCESS`
`ACFS_SEC_REALM_ADD`	`MODIFY`	Realm name	`file/user/group/command` rule name	`SUCCESS`

Table L–1 (Cont.) ACFS Security Objects Audit Events

Source Event	Command Class	Target Object	Associate Objects	Status
ACFS_SEC_REALM_DELETE	MODIFY	Realm name	file/user/group/command rule name	SUCCESS
ACFS_SEC_RULESET_CREATE	CREATE	Ruleset name	None	SUCCESS
ACFS_SEC_RULESET_DESTROY	DELETE	Ruleset name	None	SUCCESS
ACFS_SEC_RULESET_EDIT	MODIFY	Ruleset name	Rulename	SUCCESS
ACFS_SEC_RULE_CREATE	CREATE	Rule name	None	SUCCESS
ACFS_SEC_RULE_DESTROY	DELETE	Rule name	None	SUCCESS
ACFS_SEC_RULE_EDIT	MODIFY	Rule name	None	SUCCESS
ACFS_SEC_CLONE		Realm/Ruleset/Rule name	Mntpt1/Mntpt2	SUCCESS
ACFS_SEC_SAVE	BACKUP	MountPoint	None	SUCCESS
ACFS_SEC_LOAD	RESTORE	MountPoint	None	SUCCESS
ACFS_ENCR_SET	SET	MountPoint	AES-128/192/256	SUCCESS
ACFS_ENCR_VOL_REKEY	REKEY	MountPoint	AES-128/192/256	SUCCESS
ACFS_ENCR_FS_ON	ENABLE	MountPoint	Encryption	SUCCESS
ACFS_ENCR_FS_OFF	DISABLE	MountPoint	Encryption	SUCCESS
ACFS_ENCR_FILE_REKEY	REKEY	Filename	AES-128/192/256	SUCCESS
ACFS_ENCR_FILE_ON	ENABLE	Filename	None	SUCCESS
ACFS_ENCR_FILE_OFF	DISABLE	Filename	None	SUCCESS
ACFS_AUDIT_ENABLE	ENABLE	MountPoint	Audit	SUCCESS
ACFS_AUDIT_DISABLE	DISABLE	MountPoint	Audit	SUCCESS
ACFS_AUDIT_PURGE	PURGE	MountPoint	Audit trail	SUCCESS
ACFS_AUDIT_AUTO_PURGE	PURGE	MountPoint	Audit trail	SUCCESS
ACFS_AUDIT_READ	READ	MountPoint	Audit trail	SUCCESS
ACFS_AUDIT_ARCHIVE	ARCHIVE	Acfsutil command		SUCCESS
ACFS_AUDIT_SIZE	AUDIT	Acfsutil command		SUCCESS
ACFS_AUDIT_FAILURE	AUDIT	Acfsutil command		FAILURE
ACFS_SEC_ADMIN_PRIV	AUTHORIZE	Acfsutil command		FAILURE
ACFS_SEC_ADMIN_AUTH_FAIL	AUTHORIZE	Acfsutil command		FAILURE
ACFS_SYS_ADMIN_PRIV	AUTHORIZE	Acfsutil command		FAILURE
ACFS_AUDIT_MGR_PRIV	AUTHORIZE	Acfsutil command		FAILURE
ACFS_AUDITOR_PRIV	AUTHORIZE	Acfsutil command		FAILURE

Table L–1 (Cont.) ACFS Security Objects Audit Events

Source Event	Command Class	Target Object	Associate Objects	Status
ACFS_INSUFFICIENT_PRIV	AUTHORIZE	Acfsutil command		FAILURE
ACFS_ENCR_WALLET_AUTH_FAIL	AUTHORIZE	Acfsutil command		FAILURE
ACFS_SEC_CMD_FAIL	AUTHORIZE	Acfsutil command		FAILURE

Table L–2 lists the Oracle ACFS File System Objects audit events and the equivalent Oracle AVDF events.

Table L–2 ACFS File System Objects Audit Events

Source Event	Command Class	Target Object	Associate Objects	Status
ACFS_AUDIT_READ_OP	READ	Filename	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE ACFS_REALM_AUTH = SUCCESS
ACFS_AUDIT_WRITE_OP	WRITE	Filename	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE ACFS_REALM_AUTH = SUCCESS
ACFS_AUDIT_DELETE_OP	DELETE	Filename	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE ACFS_REALM_AUTH = SUCCESS
ACFS_AUDIT_OPEN_OP	OPEN	Filename	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE ACFS_REALM_AUTH = SUCCESS
ACFS_AUDIT_RENAME_OP	RENAME	Filename	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE ACFS_REALM_AUTH = SUCCESS
ACFS_AUDIT_CREATEFILE_OP	CREATE	Filename	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE ACFS_REALM_AUTH = SUCCESS
ACFS_AUDIT_MAKEDIR_OP	CREATE	DirName	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE ACFS_REALM_AUTH = SUCCESS
ACFS_AUDIT_READDIR_OP	READ	DirName	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE ACFS_REALM_AUTH = SUCCESS

Table L–2 (Cont.) ACFS File System Objects Audit Events

Source Event	Command Class	Target Object	Associate Objects	Status
ACFS_AUDIT_ OVERWRITE_OP	WRITE	Filename	Realms and command rules	ACFS_REALM_ VIOLATION = FAILURE ACFS_REALM_AUTH = SUCCESS
ACFS_AUDIT_ TRUNCATE_OP	TRUNCATE	Filename	Realms and command rules	ACFS_REALM_ VIOLATION = FAILURE ACFS_REALM_AUTH = SUCCESS
ACFS_AUDIT_ MMAPREAD_OP	READ	Filename	Realms and command rules	ACFS_REALM_ VIOLATION = FAILURE ACFS_REALM_AUTH = SUCCESS
ACFS_AUDIT_ MMAPWRITE_OP	WRITE	Filename	Realms and command rules	ACFS_REALM_ VIOLATION = FAILURE ACFS_REALM_AUTH = SUCCESS
ACFS_AUDIT_EXTEND_ OP	WRITE	Filename	Realms and command rules	ACFS_REALM_ VIOLATION = FAILURE ACFS_REALM_AUTH = SUCCESS
ACFS_AUDIT_CHOWN_OP	CHOWN	Filename/DirName	Realms and command rules	ACFS_REALM_ VIOLATION = FAILURE ACFS_REALM_AUTH = SUCCESS
ACFS_AUDIT_CHGRP_OP	CHGRP	Filename/DirName	Realms and command rules	ACFS_REALM_ VIOLATION = FAILURE ACFS_REALM_AUTH = SUCCESS
ACFS_AUDIT_CHMOD_OP	CHMOD	Filename/DirName	Realms and command rules	ACFS_REALM_ VIOLATION = FAILURE ACFS_REALM_AUTH = SUCCESS
ACFS_AUDIT_SYMLINK_ OP	SYMLINK	Filename/DirName	Realms and command rules	ACFS_REALM_ VIOLATION = FAILURE ACFS_REALM_AUTH = SUCCESS
ACFS_AUDIT_ LINKFILE_OP	LINK	Filename/DirName	Realms and command rules	ACFS_REALM_ VIOLATION = FAILURE ACFS_REALM_AUTH = SUCCESS

M

Active Directory Audit Events

Topics

About Active Directory Audit Events

This appendix maps audit event names and event ID used in the Active Directory to their equivalent values in the **command_class** and **target_type** fields in the Oracle AVDF audit record. You can use the audit events mapped here to create custom audit reports using other Oracle Database reporting products or third-party tools. See also "Oracle Audit Vault and Database Firewall Database Schemas" on page A-1 for Oracle AVDF data warehouse details that may be useful in designing your own reports.

Directory Service Audit Trail Events

Table M–1 lists the Directory Service audit trail events and their **command_class** and **target_type** mappings in the Oracle AVDF audit record.

Table M–1 Directory Service Audit Trail Events

Event ID	Source Event	command_class	target_type
1000	START_ACTIVE_DIRECTORY_DOMAIN_SERVICES_ COMPLETED	STARTUP	DIRECTORY SERVICE
1001	START_ACTIVE_DIRECTORY_DOMAIN_SERVICES_ FAILED	STARTUP	DIRECTORY SERVICE
1003	DIRLOG_DBINIT_FAILED	INITIALIZE	DATABASE
1004	SHUTDOWN_ACTIVE_DIRECTORY_DOMAIN_SERVICES_ SUCCEEDED	SHUTDOWN	DIRECTORY SERVICE
1007	DIRLOG_CHK_INIT_SUCCESS	INITIALIZE	CHECKER
1008	DIRLOG_CHK_INIT_FAILURE	INITIALIZE	CHECKER
1010	DIRLOG_NO_MEMORY_FOR_LOG_OVERRIDES	INHERIT	LOG
1016	DIRLOG_SCHEMA_NOT_LOADED	LOAD	SCHEMA
1024	DIRLOG_CHK_STOP_FAILURE	STOP	CHECKER
1054	DIRLOG_SECURITY_CHECKING_ERROR	VALIDATE	ACCESS RIGHT
1062	DOMAIN_NO_LONGER_INSTANTIATED	CREATE	DOMAIN

Table M–1 (Cont.) Directory Service Audit Trail Events

Event ID	Source Event	command_class	target_type
1066	DIRLOG_DRA_REPLICAADD_ENTRY	UPDATE	REPLICA
1067	DIRLOG_DRA_REPLICADEL_ENTRY	DELETE	REPLICA
1068	DIRLOG_DRA_UPDATEREFS_ENTRY	UPDATE	PARTITION
1070	DIRLOG_DRA_REPLICASYNC_ENTRY	SYNCHRONIZE	REPLICA
1072	DIRLOG_DRA_GETNCCH_ENTRY	SYNCHRONIZE	REPLICA
1080	NOTIFY_DS_ABOUT_CHANGES_FAILED	NOTIFY	SERVICE
1081	SEND_DP_CHANGES_FAILED	SEND	CHANGES
1082	SEND_DP_MESSAGE_WITH_CHANGES_FAILED	SEND	CHANGES
1085	SYNCHRONIZE_DIRECTORY_PARTITION_FAILED	SYNCHRONIZE	PARTITION
1089	INITIALIZE_DSP_LAYER_FAILED	INITIALIZE	PRINCIPAL
1090	DIRECTORY_PARTITION_REPLICATION_FAILED	COPY	PARTITION
1094	DISABLED_DISK_DRIVE_WRITE_CACHE	DISABLE	DRIVE
1097	REPLICATE_INVALID_DIRECTORY_PARTITION	COPY	PARTITION
1098	DIRLOG_DRA_MAIL_UPDREP_BADNC	UPDATE	REPLICA
1100	DIRLOG_DRA_RECORD_TOO_BIG_SUCCESS	UPDATE	REPLICA
1102	DIRLOG_DRA_MAIL_REQ_UPD_SENT	REQUEST	REPLICA CHANGES
1103	DIRLOG_DRA_MAIL_UPD_REP_SENT	UPDATE	REPLICA CHANGES
1104	DIRLOG_CHK_REPSTO_DEL_SUCCESS	DELETE	TOPOLOGY
1109	DIRLOG_DRA_INVOCATION_ID_CHANGED	UPDATE	INVOCATION IDENTIFIER
1111	DIRLOG_DRA_UPDATENC_PROGRESS	SYNCHRONIZE	REPLICA
1113	DIRLOG_DRA_DISABLED_INBOUND_REPL	DISABLE	REPLICATION
1114	DIRLOG_DRA_REENABLED_INBOUND_REPL	ENABLE	REPLICATION
1115	DIRLOG_DRA_DISABLED_OUTBOUND_REPL	DISABLE	REPLICATION
1116	DIRLOG_DRA_REENABLED_OUTBOUND_REPL	ENABLE	REPLICATION
1117	DIRLOG_CHK_ALL_CONNECTIONS_FOR_NC_DISABLED	DISABLE	CONNECTION
1124	DIRLOG_DRA_GET_RPC_HANDLE_FAILURE	RECEIVE	HANDLE
1125	DIRLOG_RPC_CONNECTION_FAILED	CONNECT	CALL
1138	DIRLOG_API_TRACE	EXECUTE	FUNCTION
1139	DIRLOG_API_TRACE_COMPLETE	EXECUTE	FUNCTION
1171	DIRLOG_EXIT_WITH_ACTIVE_THREADS	SHUTDOWN	DIRECTORY SERVICE
1172	DIRLOG_RPC_CONNECTION	CONNECT	SERVER
1174	DIRLOG_PRIVILEGED_OPERATION_PERFORMED	EXECUTE	OBJECT
1175	DIRLOG_PRIVILEGED_OPERATION_FAILED	EXECUTE	OBJECT
1176	DIRLOG_UNAUTHENTICATED_LOGON	LOGIN	SERVER
1177	DIRLOG_SECURITY_ATTS_MODIFIED	UPDATE	OBJECT
1194	DIRLOG_DRA_ADUPD_NC_SYNCED	SYNCHRONIZE	PARTITION

Table M–1 (Cont.) Directory Service Audit Trail Events

Event ID	Source Event	command_class	target_type
1195	DIRLOG_DRA_ADUPD_ALL_SYNCED	SYNCHRONIZE	PARTITION
1196	DIRLOG_CANT_APPLY_SERVER_SECURITY	GRANT	OBJECT
1198	DIRLOG_RECOVER_RESTORED_FAILED	RECOVER	DATABASE
1205	DIRLOG_SDPROP_OBJ_CLASS_PROBLEM	INVALIDATE	OBJECT CLASS
1209	DIRLOG_AUDIT_PRIVILEGE_FAILED	SET	AUDIT PRIVILEGE
1210	DIRLOG_ATQ_MAX_CONNECTIONS_EXCEEDED	EXCEED	CONNECTION
1211	DIRLOG_ATQ_CLOSE_SOCKET_SHUTDOWN	CLOSE	SOCKET
1213	DIRLOG_ATQ_CLOSE_SOCKET_CONTACT_LOST	CLOSE	SOCKET
1214	DIRLOG_SDPROP_NO_SD	SEARCH	SECURITY DESCRIPTOR
1215	DIRLOG_ATQ_CLOSE_SOCKET_OK	CLOSE	SOCKET
1216	DIRLOG_ATQ_CLOSE_SOCKET_ERROR	CLOSE	SOCKET
1217	DIRLOG_LDAP_NTLM_WARNING	INITIALIZE	AUTHENTICATION
1218	DIRLOG_LDAP_NEGOTIATE_WARNING	INITIALIZE	AUTHENTICATION
1219	DIRLOG_LDAP_SIMPLE_WARNING	INITIALIZE	AUTHENTICATION
1220	DIRLOG_LDAP_SSL_NO_CERT	VALIDATE	CERTIFICATE
1221	DIRLOG_LDAP_SSL_GOT_CERT	VALIDATE	CERTIFICATE
1222	DIRLOG_DRA_CERT_ACCESS_DENIED_WINERR	DENY	ACCESS
1223	DIRLOG_DRA_CERT_ACCESS_DENIED_TRUSTERR	DENY	ACCESS
1234	DIRLOG_FAILED_LOOKUP_ACCOUNT_SID	LOGIN	SERVER
1236	DIRLOG_WRONG_SERVER_NAME	VALIDATE	SERVER
1237	DIRLOG_SAM_LOOPBACK_ERROR	SEND	OPERATION
1238	DIRLOG_LDAP_SSP_ERROR	INITIALIZE	CONNECTION
1247	TRANSFER_SECURITY_PRINCIPAL_FAILED	MOVE	PRINCIPAL
1257	DIRLOG_SDPROP_DOING_PROPAGATION	EXECUTE	PROPAGATION
1258	DIRLOG_SDPROP_REPORT_ON_PROPAGATION	FINISH	PROPAGATION
1259	DIRLOG_SDPROP_STARTING	START	PROPAGATION
1260	DIRLOG_SDPROP_SLEEP	WAIT	PROPAGATION
1261	DIRLOG_SDPROP_AWAKE	NOTIFY	PROPAGATION
1262	DIRLOG_SDPROP_END_ABNORMAL	ABORT	PROPAGATION
1263	DIRLOG_SDPROP_END_NORMAL	FINISH	PROPAGATION
1264	DIRLOG_CHK_LINK_ADD_SUCCESS	UPDATE	LINK
1265	DIRLOG_CHK_LINK_ADD_FAILURE	UPDATE	LINK
1268	DIRLOG_CHK_LINK_DEL_NOTGC_SUCCESS	COPY	PARTITION
1269	DIRLOG_CHK_LINK_DEL_NOTGC_FAILURE	COPY	PARTITION
1270	DIRLOG_CHK_LINK_DEL_DOMDEL_SUCCESS	COPY	PARTITION
1271	DIRLOG_CHK_LINK_DEL_DOMDEL_FAILURE	STOP	REPLICATION
1272	DIRLOG_CHK_LINK_DEL_NOCONN_SUCCESS	COPY	PARTITION

Table M–1 (Cont.) Directory Service Audit Trail Events

Event ID	Source Event	command_class	target_type
1273	DIRLOG_CHK_LINK_DEL_NOCONN_FAILURE	STOP	REPLICATION
1274	REPLICATE_DIRECTORY_PARTITION_FAILED	COPY	PARTITION
1275	CREATE_DIRECTORY_PARTITION_FAILED	CREATE	PARTITION
1277	DIRMSG_INSTALL_FAILED_TO_CREATE_NTDSA_ OBJECT	CREATE	OBJECT
1278	DIRMSG_INSTALL_FAILED_TO_CREATE_DOMAIN_ OBJECT	CREATE	OBJECT
1279	DIRMSG_INSTALL_FAILED_TO_INIT_JET	INITIALIZE	DATABASE
1280	DIRMSG_INSTALL_FAILED_GENERAL	INSTALL	SERVER
1281	DIRMSG_INSTALL_FAILED_LDAP_CONNECT	CONNECT	CONTROLLER
1282	DIRMSG_INSTALL_FAILED_BIND	BIND	CONTROLLER
1283	DIRMSG_INSTALL_FAILED_SITE	INSTALL	SERVER
1284	DIRMSG_INSTALL_FAILED_SITE_EXIST	SEARCH	SITE
1285	DIRLOG_INSTALL_SERVER_EXISTS	VALIDATE	SERVER
1286	DIRLOG_INSTALL_FAILED_TO_DELETE_SERVER	DELETE	SERVER
1287	DIRLOG_INSTALL_DOMAIN_EXISTS	VALIDATE	DOMAIN
1288	DIRLOG_INSTALL_FAILED_TO_DELETE_DOMAIN	DELETE	PARTITION
1290	WIZARD_ACCESS_REGISTRY_FAILED	ACCESS	REGISTRY
1292	LOAD_SAM_DB_FAILED	LOAD	DATABASE
1293	CREATE_ACCOUNT_FAILED	CREATE	ACCOUNT
1294	AUTO_ENROLL_CERTIFICATE_FAILED	REGISTER	CERTIFICATE
1295	ADD_DIRECTORY_SERVICES_RESTORE_MODE_FAILED	UPDATE	RESTORE MODE
1297	ERROR_INSTALL_DOMAIN_SERVICES	INSTALL	DOMAIN SERVICE
1298	WIZARD_READ_ATTRIBUTES_FROM_DC_FAILED	READ	ATTRIBUTE
1299	SCHEMA_VALIDATION_CHECK_FAILED	VALIDATE	SCHEMA
1301	ADD_SECURITY_PRINCIPALS_TO_DS_DB_FAILED	UPDATE	PRINCIPAL
1305	SHUTDOWN_DOMAIN_SERVICES_FOR_REMOVAL_FAILED	SHUTDOWN	DIRECTORY SERVICE
1309	DIRLOG_WINSOCK_INIT_FAILED	INITIALIZE	SERVER
1317	DIRLOG_LDAP_CONNECTION_TIMEOUT	DISCONNECT	SERVICE
1318	PREPARE_SAM_DS_DEMOTION	DEMOTE	SECURITY ACCOUNT MANAGER
1319	VALIDATE_REMOVE_DOMAIN_CONTROLLER	VALIDATE	CONTROLLER
1320	AUTHENTICATE_CREDENTIAL	AUTHENTICATE	CREDENTIAL
1321	CREATE_LOCAL_ACCOUNT	CREATE	ACCOUNT
1322	CREATE_LOCAL_SAM_DATABASE	CREATE	DATABASE
1323	SET_NEW_LOCAL_SECURITY_AUTHORITY_ACCOUNT	SET	ACCOUNT
1325	REMOVE_ALL_OPERATIONS_MASTER_ROLES	DROP	ROLE
1326	REMOVE_LDAP_RPC_ACCESS	DROP	ACCESS

Table M–1 (Cont.) Directory Service Audit Trail Events

Event ID	Source Event	command_class	target_type
1327	REMOVE_COMPLETE_DS_SAM_LSA	DROP	SERVER
1328	START_INSTALL_AD_DS	INSTALL	SERVER
1329	VALIDATE_USER_SUPPLIED_OPTIONS	VALIDATE	OPTION
1330	FIND_SITE_TO_INSTALL	SEARCH	SITE
1331	EXAMINE_EXISTING_FOREST	VALIDATE	FOREST
1335	CONFIG_LOCAL_COMP_TO_HOST_DS	CONFIGURE	COMPUTER
1337	CREATE_SECURITY_ID_FOR_NEW_DOMAIN	CREATE	SECURITY IDENTIFIER
1338	REPLICATE_SCHEMA_DIRECTORY_PARTITION	COPY	PARTITION
1339	CREATE_DIRECTORY_PARTITION	CREATE	PARTITION
1340	REPLICATE_CONFIG_DIRECTORY_PARTITION	COPY	PARTITION
1342	REPLICATE_CRITICAL_DOMAIN_INFO	COPY	INFORMATION
1346	CREATE_NEW_DOMAIN_USERS_GROUPS_COMPUTER_ OBJECTS	CREATE	OBJECT
1347	COMPLETE_INSTALL_AD_DS	INSTALL	SERVER
1348	DIRLOG_BEGIN_DIR_SEARCH	SEARCH	OBJECT
1349	DIRLOG_END_DIR_SEARCH	SEARCH	OBJECT
1350	DIRLOG_BEGIN_DIR_ADDENTRY	CREATE	OBJECT
1351	DIRLOG_END_DIR_ADDENTRY	CREATE	OBJECT
1352	DIRLOG_BEGIN_DIR_REMOVE	DELETE	OBJECT
1353	DIRLOG_END_DIR_REMOVE	DELETE	OBJECT
1354	DIRLOG_BEGIN_DIR_MODIFY	UPDATE	OBJECT
1355	DIRLOG_END_DIR_MODIFY	UPDATE	OBJECT
1356	DIRLOG_BEGIN_DIR_MODIFYDN	UPDATE	OBJECT
1357	DIRLOG_END_DIR_MODIFYDN	UPDATE	OBJECT
1358	DIRLOG_BEGIN_DIR_COMPARE	COMPARE	ATTRIBUTE
1359	DIRLOG_END_DIR_COMPARE	COMPARE	ATTRIBUTE
1360	DIRLOG_DRA_REPLICASYNC_EXIT	FINISH	SYNCHRONIZATION
1362	REPLICATE_DIRECTORY_PARTITION	COPY	PARTITION
1377	INITIALIZE_TRANSPORT_FAILED	INITIALIZE	TRANSPORT
1383	DIRLOG_DRA_NO_CERTIFICATE	VALIDATE	CERTIFICATE
1384	DIRLOG_DRA_CERTIFICATE_ACQUIRED	ACQUIRE	CERTIFICATE
1390	SET_SID_FAILED_IN_SAM_DB	SET	SECURITY IDENTIFIER
1391	CONFIG_ACCOUNT_FAILED_ON_REMOTE_DC	CONFIGURE	ACCOUNT
1392	REMOVE_ACTIVE_DIRECTORY_DC_FAILED	DROP	SERVER
1411	DIRLOG_BUILD_SPN_FAILURE	CREATE	PRINCIPAL
1423	RESTORE_AD_DC_FROM_IMPROPER_BACKUP	RESTORE	CONTROLLER
1424	START_REPLICATION_CYCLE	START	CYCLE

Table M–1 (Cont.) Directory Service Audit Trail Events

Event ID	Source Event	command_class	target_type
1425	INSTALL_REPLICA	INSTALL	REPLICA
1434	DIRLOG_DB_REG_PATH_CHANGED	UPDATE	REGISTRY
1437	MISSING_CRITICAL_INFO	VALIDATE	INFORMATION
1440	CREATE_NTDS_SETTINGS_OBJECT_FAILED_ON_ REMOTE_DC	CREATE	OBJECT
1441	CREATE_NTDS_SETTINGS_OBJECT_ON_REMOTE_DC	CREATE	OBJECT
1442	DIRLOG_FAILED_TO_REMOVE_NTDSA	DROP	OBJECT
1446	DIRLOG_FAILED_TO_CREATE_RESTORE_MARKER_FILE	RESTORE	FILE
1447	DIRLOG_FAILED_TO_DELETE_RESTORE_MARKER_FILE	RESTORE	FILE
1450	DIRLOG_SDPROP_MERGE_SD_FAIL	CALCULATE	SECURITY DESCRIPTOR
1452	DIRLOG_SDPROP_ADD_SD_PROBLEM	UPDATE	SECURITY DESCRIPTOR
1458	DIRLOG_FSMO_XFER	MOVE	ROLE
1459	DIRLOG_BEGIN_DIR_FIND	SEARCH	ATTRIBUTE
1460	DIRLOG_END_DIR_FIND	SEARCH	ATTRIBUTE
1461	DIRLOG_BEGIN_LDAP_BIND	BIND	LDAP
1462	DIRLOG_END_LDAP_BIND	BIND	LDAP
1487	DIRLOG_IDL_DRS_REPLICA_SYNC_ENTRY	START	REPLICATION
1488	DIRLOG_IDL_DRS_REPLICA_SYNC_EXIT	FINISH	REPLICATION
1489	DIRLOG_IDL_DRS_GETCHG_ENTRY	START	REPLICATION
1490	DIRLOG_IDL_DRS_GETCHG_EXIT	FINISH	REPLICATION
1523	DIRLOG_SCHEMA_SD_CONVERSION_FAILED	CONVERT	SECURITY DESCRIPTOR
1524	DIRLOG_BEGIN_LDAP_REQUEST	START	OPERATION
1525	DIRLOG_END_LDAP_REQUEST	FINISH	OPERATION
1526	DIRLOG_CHK_UPDATED_SCHEDULE	UPDATE	SCHEDULE
1538	RESTORE_AD_DS_FROM_BACKUP_FAILED	RESTORE	DOMAIN SERVICE
1540	ADD_SID_TO_OBJECT_FAILED	UPDATE	SECURITY IDENTIFIER
1541	ADD_SID_TO_OBJECT_SUCCEEDED	UPDATE	SECURITY IDENTIFIER
1548	REPLICATE_DIRECTORY_PARTITION_FAILED	COPY	PARTITION
1551	SYNCHRONIZE_DIRECTORY_PARTITION	SYNCHRONIZE	PARTITION
1552	DIRLOG_DSA_NOT_ADVERTISE_DC	PUBLISH	CONTROLLER
1553	DIRLOG_ADUPD_SYNC_PROGRESS	SYNCHRONIZE	DIRECTORY PARTITION
1554	DIRLOG_ADUPD_SYNC_NO_PROGRESS	SYNCHRONIZE	DIRECTORY PARTITION
1555	DIRLOG_ADUPD_INIT_SYNC_ONGOING	RESUME	SYNCHRONIZATION
1556	DIRLOG_ADUPD_NC_GAVE_UP	STOP	SYNCHRONIZATION
1557	DIRLOG_ADUPD_NC_NEVER_SYNCED_WRITE	WRITE	PARTITION
1558	DIRLOG_ADUPD_NC_NEVER_SYNCED_READ	READ	PARTITION
1560	DIRLOG_DRA_NEW_REPLICA_FULL_SYNC	UPDATE	REPLICA

Table M–1 (Cont.) Directory Service Audit Trail Events

Event ID	Source Event	command_class	target_type
1561	DIRLOG_DRA_USER_REQ_FULL_SYNC	SYNCHRONIZE	PARTITION
1562	DIRLOG_DRA_FULL_SYNC_CONTINUED	SYNCHRONIZE	PARTITION
1564	DIRLOG_DRA_INIT_SYNCS_DISABLED	DISABLE	SYNCHRONIZATION
1569	CANCELLED_AD_DS_INSTALLATION	CANCEL	INSTALLATION
1576	DIRLOG_INHERIT_SECURITY_IDENTITY_FAILURE	INHERIT	SECURITY IDENTIFIER
1577	DIRLOG_INHERIT_SECURITY_IDENTITY_SUCCEEDED	INHERIT	SECURITY IDENTIFIER
1580	DIRLOG_DRA_REPLICATION_FINISHED	FINISH	REPLICATION
1622	DIRLOG_NSPI_BEGIN_BIND	BIND	DIRECTORY
1623	DIRLOG_NSPI_END_BIND	BIND	DIRECTORY
1642	DIRLOG_DRA_CERT_ACCESS_DENIED_NOT_DC	ACCESS	CERTIFICATE
1643	DIRLOG_SEARCH_OPERATIONS	SEARCH	DATABASE
1644	DIRLOG_SEARCH_FILTER_LOGGING	SEARCH	DATABASE
1645	DIRLOG_DRA_SPN_WRONG_TARGET_NAME	REGISTER	PRINCIPAL
1646	DIRLOG_DB_FREE_SPACE	VALIDATE	SPACE
1659	RESUMED_DIRECTORY_PARTITION_REMOVAL	REMOVE	PARTITION
1660	COMPLETED_DIRECTORY_PARTITION_REMOVAL	DROP	PARTITION
1661	REMOVE_DIRECTORY_PARTITION_OBJECTS_FAILED	DROP	OBJECT
1695	ENABLE_LINKED_VALUED_REPLICATION	ENABLE	REPLICATION
1700	PROCESS_REPLICATION_FAILED	EXECUTE	REPLICATION
1702	SYNCHRONIZE_DIRECTORY_PARTITION	SYNCHRONIZE	PARTITION
1703	SYNCHRONIZE_DIRECTORY_PARTITION	SYNCHRONIZE	PARTITION
1704	SYNCHRONIZE_DIRECTORY_PARTITION	SYNCHRONIZE	PARTITION
1710	REPLICATE_DIRECTORY_PARTITION_FAILED	COPY	PARTITION
1717	FUNCTIONAL_LEVEL_INCOMPATIBLE_WITH_OS	VALIDATE	LEVEL
1718	FUNCTIONAL_LEVEL_INCOMPATIBLE_WITH_LOCAL_DC	VALIDATE	LEVEL
1719	READ_NTDS_SETTINGS_OBJECT_FAILED	READ	OBJECT
1720	FUNCTIONAL_LEVEL_INCOMPATIBLE_WITH_OS	VALIDATE	LEVEL
1721	UPDATE_OBJECT_FUNCTIONAL_LEVEL_FAILED	UPDATE	LEVEL
1722	RAISE_OBJECT_FUNCTIONAL_LEVEL	RAISE	LEVEL
1723	RAISE_FUNCTIONAL_LEVEL_FAILED	RAISE	LEVEL
1724	UPDATE_DOMAIN_FUNCTIONAL_LEVEL_FAILED	UPDATE	LEVEL
1725	ADD_NTDS_SETTINGS_OBJECT_DENIED	UPDATE	OBJECT
1726	UPDATE_FUNCTIONAL_LEVEL_TO_INCOMPATIBLE_ VALUE	UPDATE	LEVEL
1727	RESTORE_AD_DS_FAILED_TOO_OLD_COPY	RESTORE	DOMAIN SERVICE
1728	RESTORE_AD_DS_FILES_FOR_INSTALL_FAILED	RESTORE	FILE
1746	REMOVED_DOMAIN_FROM_FOREST	DROP	DOMAIN

Table M–1 (Cont.) Directory Service Audit Trail Events

Event ID	Source Event	command_class	target_type
1750	DELETED_APPLICATION_DIRECTORY_PARTITION	DELETE	PARTITION
1752	REPLICATE_APPLICATION_DIRECTORY_PARTITION_ FAILED	COPY	PARTITION
1753	STOP_APPLICATION_DIRECTORY_PARTITION_ REPLICATION_FAILED	STOP	PARTITION
1755	STOP_DIRECTORY_PARTITION_REPLICATION_FAILED	STOP	PARTITION
1758	TRANSFER_OPERATIONS_MASTER_ROLES	MOVE	ROLE
1767	PROMOTE_DOMAIN_CONTROLLER_FAILED	PROMOTE	CONTROLLER
1769	CHECK_SECURITY_DESCRIPTOR	VALIDATE	SECURITY DESCRIPTOR
1773	INSTALL_ACTIVE_DIRECTORY_DOMAIN_SERVICES_ FAILED_FROM_RESTORED_FILES	INSTALL	DOMAIN SERVICE
1775	INITIALIZE_LDAP_MD5_AUTHENTICATION_FAILED	INITIALIZE	AUTHENTICATION
1791	REPLICATE_DIRECTORY_PARTITION_ABORTED	COPY	PARTITION
1812	INTERSITE_MESSAGING_SERVICE_INITIALIZATION_ FAILED	INITIALIZE	MESSAGING SERVICE
1838	REPLICATION_OPERATION_TAKE_LONGER_THAN_ EXPECTED	COPY	PARTITION
1861	FAILED_TO_START_RPC_SERVER	START	SERVER
1874	INSTALL_ACTIVE_DIRECTORY_DOMAIN_SERVICES_ FAILED_FROM_RESTORED_FILES	INSTALL	DOMAIN SERVICE
1877	RENAME_DOMAIN_FAILED_USER_NOT_HAVE_RIGHTS	RENAME	DOMAIN
1881	FAILED_TO_ASSIGN_NEW_DOMAIN_NAME	ASSIGN	DOMAIN
1882	AD_DS_SHUTDOWN_TO_COMPLETE_DOMAIN_RENAME_ OPERATION	SHUTDOWN	DIRECTORY SERVICE
1883	FAILED_TO_SHUTDOWN_AD_DS	SHUTDOWN	DIRECTORY SERVICE
1893	FAILED_TO_RETRIEVE_REPLICATION_EPOCH	RETRIEVE	EPOCH
1894	INSTALL_AD_DS_FAILED_FROM_RESTORED_DB_FILES	INSTALL	DOMAIN SERVICE
1901	DELETE_AUTO_ENROLLMENT_ENTRY_FOR_CERT_ SERVICES_FAILED	DELETE	ENTRY
1912	INITIALIZE_SHADOW_COPY_SERVICE_FAILED	INITIALIZE	SERVICE
1913	BACKUP_RESTORE_AD_DS_FAILED	BACKUP	DOMAIN SERVICE
1914	CANT_USE_SHADOW_COPY_SERVICE_TO_BACKUP_AD_ DS	BACKUP	SERVICE
1915	CANT_USE_SHADOW_COPY_SERVICE_TO_RESTORE_AD_ DS	RESTORE	SERVICE
1916	SHADOW_COPY_BACKUP_AD_DS_FAILED	BACKUP	DOMAIN SERVICE
1917	SHADOW_COPY_BACKUP_AD_DS_SUCCEEDED	BACKUP	DOMAIN SERVICE
1918	CANT_RESTORE_AD_DS_AS_SHADOW_COPY_TOO_OLD	RESTORE	DOMAIN SERVICE
1919	SHADOW_COPY_RESTORE_AD_DS_FAILED	RESTORE	DOMAIN SERVICE
1920	SHADOW_COPY_RESTORE_AD_DS_SUCCEEDED	RESTORE	DOMAIN SERVICE
1921	BACKUP_RESTORE_FAILED_WHILE_AD_DS_READ_ OPERATION	BACKUP	DOMAIN SERVICE

Table M–1 (Cont.) Directory Service Audit Trail Events

Event ID	Source Event	command_class	target_type
1931	AD_DS_RESTORE_FAILED_BY_SHADOW_COPY_SERVICE	RESTORE	DOMAIN SERVICE
1953	STARTED_FULL_PROPAGATION_PASS	START	PROPAGATION
1954	COMPLETED_FULL_PROPAGATION_PASS	FINISH	PROPAGATION
1956	DELETED_DIRECTORY_PARTITION	DELETE	PARTITION
1964	DIRLOG_DRA_UNAUTHORIZED_NC	DENY	REPLICATION
1965	INITIALIZE_RESTORED_DB_FILES	INITIALIZE	FILE
1966	COMPLETED_FULL_PROPAGATION_PASS	FINISH	PROPAGATION
1967	FAILED_TO_CACHE_GROUP_MEMBERSHIP	CACHE	MEMBERSHIP
1968	RAISED_DOMAIN_FUNC_LEVEL_TO_BE_COMPATIBLE_WITH_FOREST_FUNC_LEVEL	RAISE	LEVEL
1977	DIRLOG_DRA_REPLICATION_ALL_ACCESS_DENIED_DC	DENY	REPLICATION
1979	DIRLOG_SCHEMA_CLASS_DEFAULT_MOD_FAILED	CREATE	SECURITY DESCRIPTOR
1980	DIRLOG_SCHEMA_CLASS_DEFAULT_SD_MISSING	DROP	ACCESS CONTROL LIST
1981	DIRLOG_SCHEMA_CLASS_EDC_SID_FAILURE	ACCESS	SECURITY IDENTIFIER
1982	DIRLOG_SCHEMA_CLASS_DDC_REMOVE_FAILURE	DELETE	ACCESS CONTROL ENTRY
1983	DIRLOG_SCHEMA_CLASS_EDC_ACE_CREATE_FAILURE	CREATE	ACCESS CONTROL ENTRY
1987	FAILED_TO_REMOVE_LAST_DOMAIN_CONTROLLER	DROP	CONTROLLER
1989	REMOVE_APPLICATION_DIRECTORY_PARTITION_FAILED	DROP	PARTITION
1990	NOTIFY_DIRECTORY_SERVICE_FAILED_FOR_LONG_PERIOD	NOTIFY	SERVICE
1994	REFRESH_KERBEROS_SECURITY_TICKETS_FAILED	REFRESH	SECURITY TICKET
1996	AD_DS_INSTALL_REQUIRES_DOMAIN_CONFIG_CHANGES	INSTALL	DOMAIN SERVICE
1997	NOT_REPLICATED_CONFIG_CHANGES_TO_INSTALL_AD_DS	COPY	CONFIG CHANGES
1998	AD_DS_INSTALLATION_QUIT	STOP	DOMAIN SERVICE
2000	APPLIED_NTFS_SECURITY_SETTINGS	APPLY	SETTING
2001	APPLY_NTFS_SECURITY_SETTINGS_FAILED	APPLY	SETTING
2012	CANT_INSTALL_AD_DS_AS_FOREST_IS_NOT_PREPARED	INSTALL	DOMAIN SERVICE
2022	TRANSFER_OPERATIONS_MASTER_ROLES_FAILED_TO_REMOTE_DS	MOVE	ROLE
2023	REPLICATE_DIRECTORY_PARTITION_FAILED	COPY	PARTITION
2025	UNABLE_TO_GET_USER_CREDENTIAL_FOR_REQUESTED_OPERATION	GET	CREDENTIAL
2027	CREATE_APPLICATION_DIRECTORY_PARTITION_FAILED_INSUFFICIENT_PERMISSION	CREATE	PARTITION
2029	CERTIFICATE_AUTHENTICATION_FAILED	AUTHENTICATE	CERTIFICATE
2032	AD_DS_BACKUP_PREPARATION_FAILED	INITIALIZE	BACKUP

Table M–1 (Cont.) Directory Service Audit Trail Events

Event ID	Source Event	command_class	target_type
2039	RAISED_DOMAIN_FUNCTIONAL_LEVEL	RAISE	LEVEL
2040	RAISED_FOREST_FUNCTIONAL_LEVEL	RAISE	LEVEL
2043	INVALIDATED_SCRIPT_SIGNATURE	INVALIDATE	SIGNATURE
2046	CLOSED_CONNECTIONS_AS_LDAP_SEND_QUEUES_FULL	CLOSE	CONNECTION
2047	CANT_REPLICATE_CONFIG_SCHEMA_INFO	COPY	INFORMATION
2049	NO_OF_CONNECTIONS_REQUESTED_EXCEEDED_ADMIN_ LIMIT	EXCEED	CONNECTION
2050	RESTORE_AD_DS_BACKUP_FILES_FAILED	RESTORE	FILE
2055	DATABASE_RESTORE_FAILED	RESTORE	DATABASE
2060	AD_DS_DB_BACKUP_PREPARATION_FAILED	BACKUP	DATABASE
2062	AD_DS_COULD_NOT_BOOT_NORMALLY	START	DOMAIN SERVICE
2085	LDAP_SSL_CONNECTION_CANT_ESTABLISH	CREATE	CONNECTION
2097	FAILED_TO_DISABLE_OR_ENABLE_REPLICATION	CONFIGURE	REPLICATION
2101	PAUSED_NET_LOGON_SERVICE	PAUSE	SERVICE
2112	NSPI_BIND_OPERATION_COMPLETED	FINISH	BIND
2116	CANT_START_RODC_INSTALL_FROM_MEDIA_ PROMOTION	START	PROMOTION
2117	CANT_START_DC_INSTALL_FROM_MEDIA_PROMOTION	START	PROMOTION
2118	INSTALL_AD_DS_FAILED	INSTALL	DOMAIN SERVICE
2500	SHUTDOWN_AD_DS_AS_EXPIRATION_DATE_NOT_FOUND	SHUTDOWN	DIRECTORY SERVICE
2501	SHUTDOWN_AD_DS_AS_TRIAL_PERIOD_EXPIRED	SHUTDOWN	DIRECTORY SERVICE
2502	STARTED_AD_DS_TRIAL_VERSION	STARTUP	DIRECTORY SERVICE
2504	CREATED_VSS_ACCESS_CONTROL_KEY	CONFIGURE	KEY
2505	CREATE_VSS_ACCESS_CONTROL_VALUE_FAILED	CONFIGURE	VALUE
2506	ADDED_VSS_ACCESS_CONTROL_REGISTRY_KEY	UPDATE	REGISTRY
2507	INITIALIZE_SHADOW_COPY_SERVICE_FAILED	INITIALIZE	SERVICE
2508	INITIALIZE_SHADOW_COPY_SERVICE_FAILED	INITIALIZE	SERVICE
2509	OPEN_TCP_PORT_FAILED	OPEN	PORT
2510	ADD_APPLICATION_DIRECTORY_PARTITION_ REPLICA_FAILED	UPDATE	REPLICA
2511	CREATED_SERVICE_PRINCIPAL_NAME	CREATE	PRINCIPAL
2512	CANT_ESTABLISH_MUTUALLY_AUTHENTICATED_ CONNECTION	CREATE	CONNECTION
2513	SET_CONNECTION_AUTHENTICATION_PROTOCOL_ FAILED	SET	PROTOCOL
2514	UNABLE_TO_BIND_DOMAIN	BIND	DOMAIN
2515	UNABLE_TO_CRACK_ACCOUNT	SEARCH	ACCOUNT
2516	UNABLE_TO_UPDATE_SERVICE_PRINCIPAL_NAME	UPDATE	PRINCIPAL
2517	WROTE_SERVICE_PRINCIPAL_NAME	WRITE	PRINCIPAL

Table M–1 (Cont.) Directory Service Audit Trail Events

Event ID	Source Event	command_class	target_type
2521	DIRLOG_ADAM_NO_AUDITING	INITIALIZE	SYSTEM
2524	DIR_SERVICE_DETECT_DATABASE_REPLACE	UPDATE	DATABASE
2538	DIRLOG_ADAM_SERVICE_ACCOUNT_CHANGED	UPDATE	ACCOUNT
2542	DIR_SERVICE_DETECT_DATABASE_REPLACE	UPDATE	DATABASE
2550	CANNOT_INSTALL_REPLICA_IN_FOREST_USING_ LOCAL_ACCOUNT	INSTALL	REPLICA
2551	ACCOUNT_CANNOT_AUTHENTICATE_WITH_REPLICA_ SOURCE_USING_KERBEROS_MUTUAL_AUTHENTICATION	AUTHENTICATE	ACCOUNT
2553	CANNOT_INSTALL_REPLICA_IN_FOREST_USING_ BUILTIN_OR_DOMAIN ACCOUNT	INSTALL	REPLICA
2554	ACCOUNT_NAME_DOESNOT_MATCH_SOURCE_SERVER_ ACCOUNT_NAME	COMPARE	ACCOUNT
2555	ACCOUNT_CANNOT_AUTHENTICATE_WITH_REPLICA_ SOURCE_USING_NTLM_AUTHENTICATION	AUTHENTICATE	ACCOUNT
2557	UNINSTALLING_DOMAIN_SERVICES	UNINSTALL	SERVICE
2560	RECEIVED_REQUEST_TO_BEGIN_INBOUND_ REPLICATION	REQUEST	SERVICE
2561	COMPLETED_REQUEST_TO_REMOVE_LOCAL_REPLICA_ OF_DIRECTORY_PARTITION	DROP	REPLICA
2564	RECEIVED_REQUEST_TO_BEGIN_INBOUND_ REPLICATION	REQUEST	SERVICE
2567	COMPLETED_REQUEST_TO_UNINSTALL_INSTANCE	UNINSTALL	INSTANCE
2574	DS_BEGUN_UNINSTALL	UNINSTALL	SERVICE
2575	DS_COMMITTED_UNINSTALL_DATABASE	UNINSTALL	DATABASE
2579	UNINSTALL_CANT_CONNECT_ACTIVE_DIRECTORY_ DOMAIN_SERVICES	CONNECT	DOMAIN SERVICE
2580	PREPARE_DOMAIN_CONTROLLER_FOR_UNINSTALL	UNINSTALL	CONTROLLER
2581	UNINSTALL_CONNECT_NAMING_MASTER_FAILED	CONNECT	MASTER
2587	CRITICAL_FAILURE_TO_GET_USER_INPUT	GET	INPUT
2590	CONNECT_TO_SERVER_AS_DOMAIN_USER	CONNECT	SERVER
2591	CONNECT_TO_SERVER_AS_LOGGED_ON_USER	CONNECT	SERVER
2595	COMMIT_UNINSTALL_DATABASE_SUCCESSFUL	UNINSTALL	DATABASE
2603	FIND_DELETE_SERVICE_CONNECTION_POINTS_ UNDER_SERVICE_ACCOUNT_OBJECT	DELETE	POINT
2612	COMPLETE_REMOVAL_OF_ACTIVE_DIRECTORY_ DOMAIN_SERVICES	DROP	DOMAIN SERVICE
2800	DENIED_REPLICATION_CACHE_REQUEST_FOR_ SECURITY_PRINCIPAL	DENY	REQUEST
2812	FAILED_TO_GENERATE_WRITE_REFERRAL_TO_ WRITABLE_DC	CREATE	REFERRAL
2813	GENERATED_WRITE_REFERRAL_TO_WRITABLE_DC	CREATE	REFERRAL
2817	OPENED_UDP_ENDPOINT	OPEN	POINT

Table M–1 (Cont.) Directory Service Audit Trail Events

Event ID	Source Event	command_class	target_type
2818	OPEN_UDP_PORT_FAILED_FOR_EXCLUSIVE_USE	OPEN	PORT
2819	VALIDATE_NSPI_MAX_CONNECTION_LIMIT_FAILED	VALIDATE	LIMIT
2820	NSPI_MAX_CONNECTION_LIMIT_REACHED	EXCEED	CONNECTION
2828	NOT_AN_ACTIVE_DIRECTORY_DOMAIN_CONTROLLER_ ACCOUNT	VALIDATE	ACCOUNT
2834	ADD_WRITABLE_REPLICA_DIRECTORY_PARTITION_ FAILED	UPDATE	REPLICA
2840	REQUIRE_STARTUP_COM_PLUS_EVENT_SYSTEM_ SERVICE	START	SERVICE
2841	BACKUP_ACTIVE_DIRECTORY_DOMAIN_SERVICES_ FAILED	BACKUP	DOMAIN SERVICE
2842	REMOTE_PROCEDURE_CALL_TOOK_TOO_LONG_TO_ COMPLETE	FINISH	CALL
2866	ABORT_OBJECT_OPERATION_AS_LOGGING_MAX_ LIMIT_REACHED	ABORT	OPERATION
2869	CANT_START_INSTALL_FROM_MEDIA_PROMOTION_OF_ DOMAIN CONTROLLER	START	PROMOTION
2872	REPLICATE_NAMING_CONTEXT_NOT_ALLOWED_TO_ PROCEED	COPY	CONTEXT
2873	CANT_INITIALIZE_AD_DS_AS_UPDATE_DEFAULT_ SECURITY_ON_OBJECT_FAILED	UPDATE	DEFAULT SECURITY
2881	PAUSED_NET_LOGON_SERVICE	PAUSE	SERVICE
2883	DIRLOG_DRA_REPLICATION_GET_FILTERED_SET_ ACCESS_DENIED_DC	DENY	ACCESS
2884	IDENTIFIED_UNTRUSTED_CLIENT_DURING_ REPLICATION	NOTIFY	CLIENT
2885	IDENTIFIED_UNTRUSTED_CLIENT_DURING_ REPLICATION	NOTIFY	CLIENT
2887	DIRLOG_WOULD_REJECT_UNSIGNED_CLIENTS	BIND	SERVER
2888	DIRLOG_HAVE_REJECTED_UNSIGNED_CLIENTS	BIND	SERVER
2889	DIRLOG_UNSIGNED_CLIENT_DETAILS	BIND	SERVER
2890	UNABLE_TO_GAIN_AUTHORIZATION	ACQUIRE	AUTHORIZATION
2891	UPDATE_SERVICE_PRINCIPAL_NAME	UPDATE	PRINCIPAL
2892	UPDATE_SERVICE_PRINCIPAL_NAME_FAILED	UPDATE	PRINCIPAL
2893	REPLICATE_SERVICE_PRINCIPAL_NAME_FAILED	COPY	PRINCIPAL
2895	SYNCHRONIZE_ATTRIBUTES_IN_FILTERED_SET_ FAILED	SYNCHRONIZE	ATTRIBUTE
2896	DENIED_ACCESS_FOR_DIRECTORY_PARTITION_ SYNCHRONIZATION	DENY	ACCESS
104	DATABSE_STOPPED_WITH_ERROR	STOP	INSTANCE
203	STOPPED_DATABASE_BACKUP_WITH_ERROR	BACKUP	DATABASE
214	DATABASE_BACKUP_STOPPED_WITH_ERROR	BACKUP	DATABASE
217	ERROR_DURING_DATABASE_FILE_BACKUP	BACKUP	FILE

Table M–1 (Cont.) Directory Service Audit Trail Events

Event ID	Source Event	command_class	target_type
455	ERROR_IN_OPENING_LOG_FILE	OPEN	LOGFILE
471	UNABLE_TO_ROLLBACK_OPERATION_ON_DATABASE	ROLLBACK	OPERATION
481	READ_FROM_DATABASE_FILE_FAILED	READ	FILE
490	OPEN_DATABASE_FILE_FAILED_FOR_READ_WRITE_ ACCESS	OPEN	FILE
494	DATABSE_RECOVERY_FAILED	RECOVER	DATABASE
705	ONLINE_DEFRAGMENTATION_OF_DATABASE_ TERMINATED_PREMATURELY	ABORT	DEFRAGMENTATION

Security Audit Trail Events

Table M–2 lists the Security audit trail events and their **command_class** and **target_type** mappings in the Oracle AVDF audit record.

Table M–2 Security Audit Trail Events

Event ID	Source Event	command_class	target_type
4662	OPERATE_OBJECT	EXECUTE	OBJECT
4928	ESTABLISH_SOURCE_NAMING_CONTEXT	CREATE	CONTEXT
4929	REMOVE_SOURCE_NAMING_CONTEXT	DROP	CONTEXT
4930	MODIFY_SOURCE_NAMING_CONTEXT	UPDATE	CONTEXT
4931	REMOVE_DESTINATION_NAMING_CONTEXT	UPDATE	CONTEXT
4932	BEGIN_SYNCRONIZE_NAMING_CONTEXT	SYNCRONIZE	CONTEXT
4933	END_SYNCRONIZE_NAMING_CONTEXT	SYNCRONIZE	CONTEXT
4934	REPLICATE_OBJECT_ATTRIBUTES	COPY	ATTRIBUTE
4935	BEGIN_FAILURE_REPLICATION	FAIL	REPLICATE
4936	END_FAILURE_REPLICATION	FAIL	REPLICATE
4937	REMOVE_LINGERING_OBJECT_FROM_REPLICA	DROP	OBJECT
5136	MODIFY_OBJECT	UPDATE	OBJECT
5137	CREATE_OBJECT	CREATE	OBJECT
5138	RESTORE_OBJECT	RESTORE	OBJECT
5139	MOVE_OBJECT	MOVE	OBJECT
5141	DELETE_OBJECT	DELETE	OBJECT

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

W

X