Oracle® Audit Vault And Database Firewall

Auditor's Guide

Release 20
E93409-25
May 2025

Oracle Audit Vault And Database Firewall Auditor's Guide, Release 20

E93409-25

Contents

Preface

Quick Reference for Common Tasks

1 Changes in Oracle Audit Vault and Database Firewall Release 20

2 Introducing Oracle Audit Vault and Database Firewall

3 Managing Targets

4 Managing Access and Other Settings

7 Database Firewall Policies

8 Reports

9 Managing Entitlements

10 Creating Alerts

A Troubleshooting Oracle Audit Vault and Database Firewall for Auditors

B Oracle Audit Vault and Database Firewall Database Schemas

C Data Warehouse Partition

D Audit Record Fields

E Oracle Database Audit Events

J IBM DB2 Audit Events

K MySQL Audit Events

L Solaris Operating System Audit Events

M Microsoft Windows Operating System Audit Events

N Linux Operating System Audit Events

O Oracle ACFS Audit Events

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).

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 customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related Documents

See Oracle Audit Vault and Database Firewall 20.1 Books.

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.

Convention	Meaning
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.

Translation

This topic contains translation (or localization) information for Oracle AVDF User Interface and Documentation.

The Web based User Interface or the Audit Vault Server console is translated and made available in the following languages. This includes the User Interface, error messages, and help text.

- French
- German
- Italian
- Japanese
- Korean
- Spanish
- Portuguese - Brazil
- Chinese - Traditional
- Chinese - Simplified

Oracle AVDF Documentation is available in the following languages:

- English
- Japanese

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.

Targets

Viewing a List of Audit Trails for a Target

Viewing a List of Database Firewall Monitoring Points

Selecting a Firewall Policy

Viewing Audit Data Collection and Database Firewall Monitoring Details for Targets

Retrieving User Entitlement Data for Oracle Database Targets

Activating Stored Procedure Auditing

Retrieving Security Assessment Data for Oracle Database Targets

Setting a Data Retention (Archiving) Policy

Creating and Modifying Target Groups

Managing Compliance for Target Databases

Setting Access Rights for Targets and Groups

User Accounts and Access Rights

Creating Local Auditor Users

Managing User Access to Targets or Groups

Changing a User Account Type

Deleting an Auditor Account

Changing the Auditor Password

Email Notifications

Creating or Modifying an Email Distribution List

Creating or Modifying an Email Template

Status and Job Monitoring

Viewing Monitoring Point Status

Viewing Audit Trail Status

Monitoring Jobs

Audit Policies (for Oracle Databases)

Retrieving Existing Audit Policies from the Database

Retrieving Audit Policies from Multiple Oracle Databases

Specifying which Audit Policies are needed

Creating New Audit Policies

Creating Audit Policies for SQL Statements

Creating Audit Policies for Schema Objects

Creating Audit Policies for Privileges

Creating Audit Policies for Fine-Grained Auditing (FGA)

Provisioning Audit Policies to the Database

Exporting Audit Settings to a SQL Script

Provisioning Traditional Audit Policies from the Audit Vault Server

Database Firewall Policies

Creating, Copying, and Editing Database Firewall Policies

- Creating a New Database Firewall Policy
- Copying a Database Firewall Policy
- Editing a Database Firewall Policy

Defining a Database Firewall Policy

- Creating Sets
- Database Firewall Policy Rules
- SQL Statement Rule
- Database Object Rule
- Default Rule
- Blocking SQL and Creating Substitute Statements
- Configuring Policies for Login and Logout Events
- Configuring Policies for Masking Sensitive Data
- Configuring Policies for Unknown Traffic
- Configuring Database Firewall Global Policy Settings

Publishing and Deploying a Database Firewall Policy

- Publishing a Database Firewall Policy
- Deploying Database Firewall Policies from Targets Tab

Reports

- Downloading a Report in HTML or CSV Format
- Filtering Data in a Report
- Saving your Customized Reports
- Accessing Your Saved Custom Reports
- Creating a Report Schedule
- Viewing or Modifying Report Schedules
- Downloading Generated Reports in PDF or XLS Format
- Notifying Users About Generated PDF or XML Reports
- Annotating and Attesting Reports
- Creating and Uploading Your Own Custom Reports
- Activity Reports
- Compliance Reports

Entitlements

Alerts

1 Changes in Oracle Audit Vault and Database Firewall Release 20

To learn what's new in the latest release of Oracle AVDF, 20.14, see the Oracle AVDF Release Notes guide.

2 Introducing Oracle Audit Vault and Database Firewall

Before you start using Oracle Audit Vault and Database Firewwall, you should understand how its components such as targets and policies work.

2.1 Downloading the Latest Version of This Manual

Before using Oracle Audit Vault and Database Firewall, you should ensure that you have the latest version of the documentation.

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

https://docs.oracle.com/en/database/oracle/audit-vault-database-firewall/20/sigau/index.html

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

https://docs.oracle.com

2.2 Learning About Oracle Audit Vault and Database Firewall

You should understand the features, components, users, and deployment of Oracle Audit Vault and Database Firewall.

To find this information, refer to *Oracle Audit Vault and Database Firewall Concepts Guide*.

2.3 The Auditor's Role

An auditor uses the Audit Vault Server console to configure the databases or non-databases you are monitoring with Oracle Audit Vault and Database Firewall.

The auditor uses the Audit Vault Server console to configure the following:

- **Targets** - For each target you are monitoring, the Oracle Audit Vault and Database Firewall administrator must configure a target in the Audit Vault Server. As an auditor, you can then specify audit and/or firewall policies for the target, as well as other requirements.
- **Database Firewall Policies** - For any supported database, you can use the Database Firewall and design a firewall policy based on SQL statements from your targets.
- **Audit Policies** - For Oracle databases, you can use Oracle Audit Vault and Database Firewall to design audit policies and provision them to the database.
- **Alerts** - You can create simple or complex alerts based on conditions you specify for the targets you are monitoring. You can also specify alert notifications using email templates.
- **Audit Trails** - For any target type, you can monitor the status of audit trails and see audit reports.
- **Reports** - You can schedule and generate a number of audit and firewall reports in Oracle Audit Vault and Database Firewall, create report notifications, as well as add your own customized reports.

Auditor Roles in Oracle Audit Vault and Database Firewall

There are three auditor roles in Oracle Audit Vault and Database Firewall, with different access levels:

- **Super Auditor** - This role has access to all targets and can grant access to specific 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 targets to which they have been granted access by a super auditor.
- **Readonly Auditor** - This role has read only access to targets, audit trails, Database Firewall monitoring points, dashboard, reports, charts, access rights data, and can add filters.

> **See Also:**
>
> - Understanding Targets
> - Database Firewall Policies
> - Creating Audit Policies for Oracle Databases
> - Creating Alerts
> - Viewing a List of Audit Trails for a Target
> - Reports
> - Managing Access and Other Settings

2.4 Understanding Targets

A target is any supported database or non-database that you monitor with Oracle Audit Vault and Database Firewall.

Targets can be monitored by the Audit Vault Agent, the Database Firewall, or both.

The Oracle Audit Vault and Database Firewall administrator creates and configures targets, providing host addresses, usernames, passwords, and other necessary information.

For a target to be monitored by Database Firewall, the administrator must configure the Database Firewall, and also configure a monitoring point for every target.

Once 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 by a Database Firewall:
  - Design and apply a firewall policy
  - View the status of configured monitoring points
- If the 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 target groups for access control purposes. Super auditors grant auditors access to individual targets or to target groups.

> **See Also:**
>
> Managing Targets

2.5 Understanding Firewall Policies

An Oracle Audit Vault and Database Firewall policy monitors Oracle Database statements, objects, privileges, or fine-grained auditing.

> **See Also:**
>
> - Chapter 4 of *Oracle Audit Vault and Database Firewall Concepts Guide* for detailed information.
> - Database Firewall Policies

2.6 Understanding Audit Policies and Audit Data Collection

Learn about how audit policies manage audit data collection.

> **See Also:**
>
> - Chapter 3 of *Oracle Audit Vault and Database Firewall Concepts Guide* for detailed information
> - Creating Audit Policies for Oracle Databases

2.7 Requirements for Collecting Audit Data from Targets

Oracle Audit Vault and Database Firewall targets include Oracle Database, SQL Server, Sybase ASE, and IBM DB2 databases.

2.7.1 Requirements for Oracle Database

You should ensure that auditing is enabled in the target database and that it uses the recommended audit settings.

2.7.1.1 Ensuring That Auditing Is Enabled in the Target Database

Oracle Audit Vault and Database Firewall can collect audit data from the 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.

2.7.1.2 Using Recommended Audit Settings in the Target Database

After your database administrator checks that auditing is enabled, Oracle recommends that you set several areas of auditing in the database.

These areas that you must enable are as follows:

- **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;`

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

Ensure that auditing is enabled in these databases.

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

2.8 Configuring Alerts and Notifications

Oracle Audit Vault and Database Firewall 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 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.

> **See Also:**
>
> Creating Alerts

2.9 Generating Reports

As an Oracle Audit Vault and Database Firewall auditor, you can generate various audit reports for the 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 Audit Vault and Database Firewall also lets you browse and customize report data interactively, and upload your own custom reports created with third party tools.

See Also:

- Reports
- Managing Entitlements

2.10 Creating Users and Managing Access

A super auditor creates auditor accounts, and manages auditor access to targets and target groups.

See Also:

Managing Access and Other Settings for information on these functions.

2.11 Logging in and Understanding the Audit Vault Server Console UI

After you log in to the Audit Vault Server Console, you can work with various tabbed pages and lists of objects.

2.11.1 Logging in to the Audit Vault Server Console

To log in to the Audit Vault Server console, you must have a valid user name and password.

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.

2.11.2 Understanding the Tabs in the Audit Vault Server Console UI

An auditor or super auditor can see the auditor's dashboard on the home page and the functions that are available for the auditor roles.

Home page

The **Home** tab on the console has the following sections:

- **Targets**

- **Security assessment for Oracle databases**
- **Security assessment drift graph** (Starting in Oracle AVDF 20.11, this section will be included.)
- **All activity** (Starting in Oracle AVDF 20.11, this section will be omitted.)
- **Alerts**
  - **Open alerts**
  - **Alerts by severity**
  - **Top 5 targets by alerts**
  - **Top 5 alert policies by volume**

There is an option to filter the display by time period.

Other tabs

- **Audit Insights** - See a summarized view of details about your targets, users, and policies, including total counts and top five activity and sensitive data details. You can drill down from the summary view and charts to the detailed activity reports. In rare cases, the summary view may be out of sync with the charts.
- **Targets** - Set firewall, audit, and data retention policies for each target; manage entitlement snapshots; set up target groups; see audit trails and monitoring points.
- **Policies** - Manage audit and firewall policies, and configure alerts.
- **Alerts** - Manage alerts.
- **Reports** - Generate default reports, schedule reports, customize reports online, and upload your custom reports.
- **Settings** Change your password, create and manage email distribution lists, configure email notification templates for alerts and reports, view audit trail and monitoring point status, manage user accounts and access, and view job status.

2.11.3 Working with Lists of Objects in the UI

Throughout the Audit Vault Server UI, you will see lists of objects such as reports, users, targets, firewall policies, and so on.

You can filter and customize any of these lists of objects in the same way as you can for Oracle Audit Vault and Database Firewall reports. This section provides a summary of how you can filter and custom the display of lists of objects.

> **See Also:**
>
> Filtering Data in a Report

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

1. Click on the report, list, or column heading.
2. You can customize the list, by selecting any of the following available options:
   - Sort Ascending
   - Sort Descending

- Hide Column
- Control Break

3

Managing Targets

You can view and change target settings, create and modify target groups, manage compliance settings, and set access rights to targets and groups.

3.1 About Managing Targets

Targets are created by an Oracle Audit Vault and Database Firewall administrator.

A target is created for each database or other supported audit source for which you want to retrieve audit data, and for a database you want to monitor with a Database Firewall.

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

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

- View and sort the list of targets.

  > **See Also:**
  >
  > Working with Lists of Objects in the UI

- View and access the following for each target:
  - Audit Trails
  - Database Firewall Monitoring
  - Target Groups
  - Access Rights
  - User Entitlements Snapshots

3.2 Viewing and Changing Settings for a Target

You can view and change settings such as policy settings, entitlement data, or a list of audit trails for a target.

3.2.1 Viewing Audit Data Collection and Database Firewall Monitoring Details for Targets

You can view audit data collection and database firewall monitoring details for each target on the **Targets** tab.

1. Log into the Audit Vault Server console as an auditor.
2. Click the **Targets** tab.
3. Select a target from the list.

On the target details page, you can view the following information about the target:

- **Connect String**
- **Description**
- **Retention Policy** displays the data retention policy that is currently in effect for the target. You can also select a new policy here.
- **Audit Data Collection** displays details about the current audit trails that are configured for the target. Details include the audit trail location, trail type, status, name of the agent, time the collection was last started, and time until which data was collected.
- For database targets, the **Database Firewall Monitoring** displays details about the current database firewall monitoring points that are configured for the target. Details include the connection details, database firewall name, status, traffic source, proxy port, and deployment mode. You can also view and change the database firewall monitoring policy here.

Related Topics

- Logging in to the Audit Vault Server Console
  To log in to the Audit Vault Server console, you must have a valid user name and password.
- Creating Audit Policies for Oracle Databases
  You can retrieve and provision audit configurations for an Oracle Database.
- Database Firewall Policies
  You can create and manage Database Firewall policies.

3.2.2 Scheduling the Retrieval of Audit Settings for an Oracle Database

To retrieve audit policy settings for an Oracle Database, schedule an audit policy retrieval job for the target.

After patching to Oracle AVDF 20.12, you will need to

1. Rerun the Oracle privileges script for successful audit policy retrieval for container database targets. For more information see Oracle Database Setup Scripts.
2. Retrieve audit policies before provisioning or viewing audit policies. For more information see Retrieving and Modifying Audit Policies from an Oracle Database

1. Log in to the Audit Vault Server console as an auditor.
2. Click the **Targets** tab.
3. Click the **Schedule Retrieval Jobs** icon for the target.
4. On the Schedule Retrieval Jobs page, select one of the following options under **Audit Policy**:
   - To run the job immediately, select **Retrieve Immediately**.
   - To schedule the job or change an existing schedule, follow these steps:
     a. Select **Create/Update Schedule**.
     b. Select **Enable**.
     c. Enter the start date and time and the repetition frequency.
5. Click **Save**.

Related Topics

- Logging in to the Audit Vault Server Console
  To log in to the Audit Vault Server console, you must have a valid user name and password.
- Monitoring Jobs
  You can see the status of Audit Vault Server jobs, such as report generation, and user entitlement, or audit policy retrieval from targets.
- Managing Targets
  You can view and change target settings, create and modify target groups, manage compliance settings, and set access rights to targets and groups.

3.2.3 Retrieving User Entitlement Data for Oracle Database Targets

To retrieve data for user entitlement snapshots, submit or schedule a user entitlement retrieval job for an Oracle Database target.

1. Log in to the Audit Vault Server console as an auditor.
2. Click the **Targets** tab.
3. Click the **Schedule Retrieval Jobs** icon for the target.
4. On the Schedule Retrieval Jobs page, select one of the following options under **User Entitlements**:
   - To run the job immediately, select **Retrieve Immediately**.
   - To schedule the job or change an existing schedule, follow these steps:
     a. Select **Create/Update Schedule**.
     b. Select **Enable**.
     c. Enter the start date and time and the repetition frequency.
5. Click **Save**.

> **Note:**
>
> All user entitlement snapshots will be purged after 18 months from the time of data retrieval.

Related Topics

- Working With Entitlement Snapshots and Labels
  Learn about working with entitlement snapshots and labels.
- Logging in to the Audit Vault Server Console
  To log in to the Audit Vault Server console, you must have a valid user name and password.
- Monitoring Jobs
  You can see the status of Audit Vault Server jobs, such as report generation, and user entitlement, or audit policy retrieval from targets.

3.2.4 Retrieving Security Assessment Data for Oracle Database Targets

To retrieve data for the security assessment reports, submit or schedule the security assessment retrieval job for an Oracle Database target.

When an Oracle Database is registered as a target in Oracle AVDF, the first security assessment job is submitted automatically. You can then manually submit the job to run immediately or schedule it to run at a specified frequency, such as weekly or monthly.

> **Note:**
>
> All assessment data will be purged after 18 months from the time of data retrieval.

For implementing Database Security Posture Management (DSPM), it is recommended to schedule the Security Assessment retrieval job for each target.

To create or change a security assessment retrieval job:

1. Log in to the Audit Vault Server console as an auditor.
2. Click the **Targets** tab.
3. Click the **Schedule Retrieval Jobs** icon for the target.
4. On the Schedule Retrieval Jobs page, select one of the following options under **Security Assessment**:
   - To run the job immediately, select **Assess Immediately**.
   - To schedule the job or change an existing schedule, follow these steps:
     a. Select **Create/Update Schedule**.
     b. Select **Enable**.
     c. Enter the start date and time and the repetition frequency.
5. Click **Save**.

Related Topics

- Assessment Reports
  The assessment reports capture security assessment data from Oracle Databases that are configured as targets in Oracle Audit Vault and Database Firewall (Oracle AVDF) 20.9 and later.
- Logging in to the Audit Vault Server Console
  To log in to the Audit Vault Server console, you must have a valid user name and password.
- Monitoring Jobs
  You can see the status of Audit Vault Server jobs, such as report generation, and user entitlement, or audit policy retrieval from targets.

3.2.5 Retrieving Sensitive Objects for Oracle Database Targets

To identify privileged users and sensitive data for data discovery, submit or schedule the sensitive data retrieval job for an Oracle Database target.

When an Oracle Database is registered as a target in Oracle AVDF, the first data discovery job is submitted automatically. You can then manually submit the job to run immediately or schedule it to run at a specified frequency, such as weekly or monthly.

To create or change a sensitive data discovery job:

1. Log in to the Audit Vault Server console as an auditor.
2. Click the **Targets** tab.
3. Click the **Schedule Retrieval Jobs** icon for the target.
4. On the Schedule Retrieval Jobs page, select one of the following options under **Sensitive Objects**:
   - To run the job immediately, select **Discover Immediately**.
   - To schedule the job or change an existing schedule, follow these steps:
     a. Select **Create/Update Schedule**.
     b. Select **Enable**.
     c. Enter the start date and time and the repetition frequency.
   - To disable the schedule, follow these steps:
     a. Select **Create/Update Schedule**.
     b. Select **Disable**.

     > **Note:**
     >
     > Disabling the schedule does not revoke the user privileges for data discovery on the Oracle Database. Disabling the schedule only stops the schedule and prevents the sensitive data from updating.
5. Click **Save**.

Related Topics

- Managing Global Sets/Data Discovery
  Oracle AVDF 20.9 introduced Data Discovery which allowed the creation of global Privileged User and Sensitive Object sets on Oracle Database targets. In Oracle AVDF 20.10 this functionality was renamed to Global Sets and expanded to additionally allow the creation of global IP Address, OS User, Client Program, and Database User sets.
- Logging in to the Audit Vault Server Console
  To log in to the Audit Vault Server console, you must have a valid user name and password.

3.2.6 Activating Stored Procedure Auditing

To retrieve data for the stored procedure auditing reports, schedule the stored procedure auditing retrieval job for a database target.

1. Log in to the Audit Vault Server console as an auditor.
2. Click the **Targets** tab.
3. Click the **Schedule Retrieval Jobs** icon for the target.
4. Under **Stored Procedure Auditing**, follow these steps:

   a. Select **Create/Update Schedule**.
   b. Select **Enable**.
   c. Enter the start date and time and the repetition frequency.
5. Click **Save**.

> **Note:**
>
> See *Oracle Audit Vault and Database Firewall Administrator's Guide* for information about collecting stored procedure changes from a target database. An Oracle Audit Vault and Database Firewall administrator must run scripts to set up the correct user privileges on the target database.

Related Topics

- Stored Procedure Changes
  The **Stored Procedure Changes** auditing reports allow you to audit changes to stored procedures on target databases.
- Logging in to the Audit Vault Server Console
  To log in to the Audit Vault Server console, you must have a valid user name and password.
- Monitoring Jobs
  You can see the status of Audit Vault Server jobs, such as report generation, and user entitlement, or audit policy retrieval from targets.

3.2.7 Viewing a List of Audit Trails for a Target

An Oracle Audit Vault and Database Firewall administrator starts and stops audit trails.

As an auditor, you can view lists of audit trails for targets you have access to. You can see the trails collected for one or more targets.

1. Log into the Audit Vault Server console as an *auditor*.
2. Click **Targets** tab.
3. Click **Audit Trails** in the left navigation menu.
4. Select a target from the list displayed. The details pertaining to the specific target is displayed on the screen.
5. Scroll down. The **Audit Data Collection** tab is selected by default.

   The audit trails for the target are listed in a table with the following columns:

   - **Audit Trail Location**
   - **Audit Trail Status**
   - **Audit Trail Type**
   - **Collection Agent**
   - **Last Start At**
6. Optionally, click on the column name title for the following options:
   - **Sort Ascending**
   - **Sort Descending**

- **Hide Column**
- **Control Break**

There is search field and other options available.

> **See Also:**
>
> Logging in to the Audit Vault Server Console

3.2.8 Selecting a Firewall Policy

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

1. Log into the Audit Vault Server console as an *auditor*.
2. Click **Policies** tab
3. Click **Database Firewall Policies** tab in the left navigation menu.
4. A list of **User-defined Database Firewall Policies** and **Pre-defined Database Firewall Policies** are displayed on the screen.
5. Click on a specific target to view the firewall policy defined. You can make changes to the policy here from this screen.

> **See Also:**
>
> - Database Firewall Policies for detailed information on firewall policies.
> - Logging in to the Audit Vault Server Console

3.2.9 Viewing a List of Database Firewall Monitoring Points

An Oracle Audit Vault and Database Firewall administrator creates monitoring points for database targets monitored by Database Firewall.

As an auditor, you can see the Database Firewall monitoring points configured for the database targets you have access to. You can see the monitoring points for one target or for all your targets.

3.2.9.1 Viewing a List of Monitoring Points for a Database Target

You can access a list of monitoring points for a database target.

1. Log into the Audit Vault Server console as an *auditor*.
2. Click on **Targets** tab.

   The **Targets** sub tab in the left navigation menu is selected by default. The main page lists all the targets configured.
3. Select a specific target.

4. Scroll down and click on **Database Firewall Monitoring** sub tab. It contains a list of all the Database Firewall monitoring points associated with this target. This section is not visible if the target is not a database.

> **See Also:**
>
> Logging in to the Audit Vault Server Console

3.2.9.2 Viewing a List of Monitoring Points for All Your Target Databases

You can access a list monitoring points configured for all your database targets.

1. Log in to the Audit Vault Server console as an *auditor*.
2. Click on **Targets** tab.
3. From the left navigation menu, click **Database Firewall Monitoring**.
4. The main page lists all the targets and the status of the corresponding Database Firewall monitoring points. Click the name of the specific target to see its details.

> **See Also:**
>
> Logging in to the Audit Vault Server Console

3.2.10 Setting a Data Retention (Archiving) Policy

The data retention policy for a target determines how long audit data is retained for that target.

An Oracle Audit Vault and Database Firewall administrator creates retention policies, and an auditor selects one of the available policies to assign to a target. If you do not select a retention policy for a target, the default retention policy will be used (12 months retention online and 12 months in archives before purging). Do not set the retention policy after data collection has started from the target. After the retention period is reached, the archived data is purged and cannot be retrieved. A new retention policy takes effect as of the date you select the policy, but does not apply to existing data.

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

   The **Targets** sub tab in the left navigation menu is selected by default. The main page lists all the targets configured.
3. Select a target from the list.
4. The **Retention Policy** field displays the duration of the retention and archival policy for the specific target.
5. To set or change the retention policy, click the edit icon next to the **Retention Policy** field. Select from the available retention policies.
6. Click **Save**.

See Also:

- *Oracle Audit Vault and Database Firewall Administrator's Guide* for information on configuring retention (archiving) policies.
- Logging in to the Audit Vault Server Console

3.3 Creating and Modifying Target Groups

You can create and modify a named group of targets.

3.3.1 About Target Groups

A super auditor can organize multiple targets into a group to grant auditor access to them in one operation instead of individually.

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

3.3.2 Creating and Modifying Target Groups

You must be a super auditor to create and modify target groups.

Creating a target group

1. Log in to the Audit Vault Server console as a super auditor.
2. Click **Targets** tab.
3. Click **Target Groups** tab in the left navigation menu. A list of **User-define Groups** and **Pre-configured Groups** are displayed on the screen.
4. Click **Create** button in the top right corner.
5. In the **Create Target Group** dialog, do the following:

Release Oracle AVDF 20.1 and 20.2	Release Oracle AVDF 20.3 and later
a. **Name** field: Enter a name for the target group. b. **Description**: Optionally, enter a description for this target group. c. Under **Members** section, select one or more members by clicking the check box against the member name. d. Click the **Add** button.	a. **Group Name** field: Enter a name for the target group. b. **Description**: Optionally, enter a description for this target group. c. Under **Members** section, select one or more members by moving them from the **Available** column to **Selected** column. You can also search for the targets in the field below the **Members** section using the target name. d. To remove the targets, select one or more members and move them back to

	the **Available** column from the **Selected** column.

6. Click **Save**.

Modifying a target group

1. Log in to the Audit Vault Server console as a super auditor.
2. Click **Targets** tab.
3. Click **Target Groups** tab in the left navigation menu. A list of **User-define Groups** and **Pre-configured Groups** are displayed on the screen.
4. Click the name of the target group to modify.
5. In the **Modify Target Group** dialog, perform any of the following modifications:

Release Oracle AVDF 20.1 and 20.2	Release Oracle AVDF 20.3 and later
a. Change the **Name** of the target group. b. Optionally edit the **Description**. c. Under the **Members** section, add or remove members by selecting the check box against the member. d. Click **Add** or **Remove** buttons accordingly.	a. Change the **Group Name**. b. Optionally edit the **Description**. c. Under the **Members** section, add or remove members by moving them in between the **Available** and **Selected** columns. You can also search for the targets in the field below the **Members** section using the target name.

6. Click **Save**.

> **See Also:**
>
> - Working with Lists of Objects in the UI
> - Logging in to the Audit Vault Server Console

3.4 Managing Compliance for Target Databases

To ensure that the correct compliance reports are available for target databases, you add those targets to the appropriate preconfigured group in the Audit Vault Server.

To assign a target to a compliance group:

1. Log in to the Audit Vault Server console as an *auditor*.
2. Click **Targets** tab.
3. Click **Target Groups** tab in the left navigation menu.

   A list of **User-defined Groups** and **Pre-configured Groups** are displayed on the screen.
4. In the **Pre-configured Groups** section, click on a specific group name.
5. In the **Modify Target Group** dialog:

Release Oracle AVDF 20.1 and 20.2	Release Oracle AVDF 20.3 and later
a. Select the target databases to add to this compliance group. b. Select the targets and then click **Remove**, to remove a target database from the compliance group.	a. Select the target databases to add to the compliance group by moving them from the **Available** column to the **Selected** column. b. Select the target databases to remove from the compliance group by moving them from the **Selected** column to the **Available** column.

6. Click **Save**.

> **See Also:**
>
> - Compliance Reports for more information on compliance reports.
> - Logging in to the Audit Vault Server Console

3.5 Setting Access Rights for Targets and Groups

If you have the super auditor role in Oracle Audit Vault and Database Firewall, you can set access rights for targets and groups.

Only auditors that have been granted access to specific targets or groups will be able to see them or data related to them. You can manage access by target or group, or by user.

> **See Also:**
>
> Managing User Accounts and Access for instructions.

4

Managing Access and Other Settings

Types of access and other settings refers to areas such as user accounts and privileges or creating report templates.

4.1 Managing User Accounts and Access

A super user can manage user accounts and access.

4.1.1 About Oracle AVDF Auditor Accounts and Passwords

Learn about Oracle AVDF auditor user accounts and passwords.

There are three types of auditor accounts in Oracle Audit Vault and Database Firewall:

- **Super Auditor:**
  - Creates user accounts for super auditors and auditors
  - Has auditor access to all targets and target groups
  - Grants auditor access to targets or target groups to auditors
- **Auditor:** Has access to specific targets or target groups granted by a super auditor
- **Readonly Auditor:** Has readonly access to:
  - Target database details as granted to them by the **Super Auditor**
  - Audit trail details
  - Database Firewall monitoring points
  - Dashboard data on the **Home** page, including the ability to view chart data and add filters
  - User entitlement, target database, and target database group access details
  - All reports and report schedules. **Compliance Reports** and **Generated Reports** for specific target databases are only visible to the **Readonly Auditor** if they have been granted access to the target database by the **Super Auditor**
  - All alerts and alert details

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.

4.1.2 Creating Local Auditor Users

Learn how to create user accounts with auditor privileges.

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

To create an auditor account in Oracle Audit Vault and Database Firewall:

1. Log in to the Audit Vault Server console as a *super auditor*.
2. Click the **Settings** tab.
   The **Manage Auditors** subtab on the main page is selected by default.
3. Click **Add** in the top, right corner.
4. In the **Add Auditor** dialog box, select **Local AVDF User**.
5. For **Local AVDF User**, enter the details to create a database auditor.
6. Enter the newly created **Auditor Name**.
7. Select the **Auditor Type**.
8. Enter the **Password** and **Re-type Password**.
   Oracle Audit Vault and Database Firewall does not accept user names with quotation marks, such as `"jsmith"`.
9. Click **Save**.

Related Topics

- About Oracle AVDF Auditor Accounts and Passwords
  Learn about Oracle AVDF auditor user accounts and passwords.
- Logging in to the Audit Vault Server Console
  To log in to the Audit Vault Server console, you must have a valid user name and password.

4.1.3 Creating New SSO Users

To create new users for single sign-on (SSO) authentication, you enter the user name and the auditor type.

1. Log in to the Audit Vault Server console as a `super auditor`.
2. Click the **Settings** tab.
3. On the **Manage Auditors** subtab, click **Add**.
4. In the dialog box, select **Single Sign-On**.
5. Enter the SSO user name.

   Allowed characters include uppercase letters, lowercase letters, numbers, and symbols (@.-_!^~+%). The total length of the SSO user name can't exceed 127 characters.

> **Note:**
>
> Though AVDF accepts uppercase and lowercase letters, it will store the user name in only uppercase. Microsoft performs a case in-sensitive comparison of the user names.

6. Select the auditor type, **Auditor**, **Readonly Auditor**, or **Super Auditor**.
7. Click **Save**.

Related Topics

- Configuring Single Sign-On (SSO) for Audit Vault Server Console Users

4.1.4 Viewing the Status of Auditor User Accounts

Learn how to view the status of auditor user accounts.

As a super auditor, you can view the status of auditor accounts by clicking the **Settings** tab. The Manage Auditors page lists all auditor and super auditor accounts, their status, and password expiry dates.

4.1.5 Managing User Access to Targets or Groups

Learn to manage user access to targets and target groups.

4.1.5.1 About Managing User Access

Learn about managing user access.

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

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

- Modify a 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 targets or groups.

4.1.5.2 Controlling Access by User

Learn about controlling user access to targets.

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

1. Log in to the Audit Vault Server console as a super auditor.
2. Click **Settings**. The **Manage Auditors** page displays existing users and the targets or groups to which they have access.
3. Click the name of the user account that you want to modify.

   The **Modify Auditor** page appears.
4. In the **Targets & Target Groups** section:

Release Oracle AVDF 20.1 and 20.2	Release Oracle AVDF 20.3 and later

a. Select the access rights to which you want to grant or revoke access for this user. b. Click **Grant Access** or **Revoke Access**. A check mark indicates access granted. An cross mark ("x") indicates access revoked. A green check mark indicates that access is granted.	a. Select the access rights to which you want to grant or revoke for this user. You can also search for the access rights in the field under **Targets & Target Groups**. b. Choose the access rights in the **Available** column and move them to the **Selected** column, to grant access. Choose the access rights in the **Selected** column and move them to the **Available** column, to revoke access.

5. Click **Save**.

> **See Also:**
>
> Logging in to the Audit Vault Server Console

4.1.5.3 Controlling Access by Target or Group

Learn about controlling access to targets or target groups.

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

1. Log in to the Audit Vault Server console as a super auditor.
2. Click **Targets** tab.
3. Click **Access Rights** tab in the left navigation menu.
4. Click the name of the target or target group for which you want to redefine access rights.

   The **Modify Access** dialog for the specific target or group appears. It lists the user access rights to the target or group. Super auditors have access by default.
5. In the **Modify Access** dialog, select the users for which you want to grant or revoke access to this target or group.

Release Oracle AVDF 20.1 and 20.2	Release Oracle AVDF 20.3 and later
a. Select the users for which you want to grant or revoke access to the targets or groups. b. Click **Grant** or **Revoke** button. A green check mark indicates access granted. A red cross mark (X) indicates access revoked.	a. Select the users for which you want to grant or revoke access to the targets or groups. You can also search for the users in the field. b. Choose the access rights in the **Available** column and move them to the **Selected** column, to grant access. Choose the access rights in the **Selected** column and move them to the **Available** column, to revoke access.

6. Click **Save**.

See Also:

Logging in to the Audit Vault Server Console

4.1.6 Changing a User Account Type

Learn how to change auditor user account type.

You can change an auditor account type between **Readonly Auditor**, **Auditor**, and **Super Auditor**. If a user's account type is changed from **Auditor** or **Readonly Auditor** to **Super Auditor**, that user will have access to all targets and target groups. A user can only be assigned one auditor account type at a time.

To change a user account type in Oracle Audit Vault and Database Firewall:

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 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** dialog, against the **Type** field, click on the edit icon.
5. In the **Type** drop-down list, select the new auditor type.
6. If you changed the type from **Super Auditor** to **Auditor** or **Readonly Auditor**, grant or revoke access to any targets or groups as necessary for this user.

Release Oracle AVDF 20.1 and 20.2	Release Oracle AVDF 20.3 and later
a. Select the targets or groups to which you want to grant or revoke access. b. Click **Grant** or **Revoke**. A green check mark indicates access granted. A red cross mark (X) indicates that access is revoked.	a. Select the targets or groups to which you want to grant or revoke access. You can also search for the targets or groups in the field under **Targets & Target Groups**. b. Choose the targets and groups in the **Available** column and move them to the **Selected** column, to grant access. Choose the targets and groups in the **Selected** column and move them to the **Available** column, to revoke access.

7. Click **Save**.

See Also:

Logging in to the Audit Vault Server Console

4.1.7 Changing the Auditor Password

Learn how to change the password of an auditor.

Auditors can change their own password. A **Super Auditor** can also change the password of other auditors. If a **Super Auditor** changes the password of another auditor, then the password automatically expires immediately after it is changed.

> **See Also:**
>
> About Oracle AVDF Auditor Accounts and Passwords

4.1.7.1 Changing Your Own Password

You can change your own password any time.

1. Log in to the Audit Vault Server console as an auditor.
2. In the upper right corner, to the right of your login name, select the menu icon.
3. Select **Change Password** from this menu.
4. In the **Change Password** window, enter the following fields:
   a. **Current Password**
   b. **New Password**
   c. **Re-enter New Password**
5. Click **Save**.

4.1.7.2 Changing the Password of Another Auditor

Learn how to change the password of another auditor as a **Super Auditor**.

A **Super Auditor** can change the passwords of other auditors. However, the password automatically expires immediately after it is changed by the **Super Auditor**. The auditor must follow the instructions in the topic Changing the Expired Password of an Auditor.

1. Log in to the Audit Vault Server as **Super Auditor**.
2. Click the **Settings** tab. The **Manage Auditors** tab in left navigation menu is selected by default.
3. Under **Manage Auditors**, click the name of the auditor whose password you want to change.
4. In the **Modify Auditor** window, click **Change Password**.
5. In the **Change Password** window, enter the following fields:
   a. **New Password**
   b. **Re-enter New Password**
6. Click **Save**.

4.1.7.3 Changing the Expired Password of an Auditor

Your password might be expired if a **Super Auditor** changes your password, or if it passes the password expiry date.

For Oracle AVDF release 20.4 or earlier, follow these steps:

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Switch to the `dvaccountmgr` user.

   ```
   su - dvaccountmgr
   ```
3. Start SQL*Plus without the user name and password.

   ```
   sqlplus /
   ```
4. If the account is locked, run the following command to unlock the account:

   ```
   alter user <user name> account unlock;
   ```
5. Run the following command to change the password:

   ```
   alter user <username> identified by <new_password>;
   ```

For Oracle AVDF release 20.5 or later, follow these steps:

1. Log in to AVCLI with your auditor user name.
2. AVCLI prompts to enter the password. Enter the expired password.

   The following message is displayed:

   ```
   The password has expired. Enter the new password:
   ```
3. Enter the new password of your choice. Follow the password requirements.

   The following message is displayed:

   ```
   Re-enter password:
   ```
4. Re-enter the new password.
5. If the following message is displayed, then you have successfully logged in to AVCLI with the new password, and your account is active again:

   ```
   Connected to:
           Oracle Audit Vault Server - Version : 20.x.0.0.0
   ```

> **Note:**
>
> If your attempt to log in fails for 3 times or more, then your account gets locked. You need to unlock your account and retry the above mentioned steps.

> **See Also:**
>
> - Logging in to AVCLI
> - About Oracle AVDF Auditor Accounts and Passwords
> - Unlocking User Accounts

4.1.8 Deleting an Auditor Account

As a **Super Auditor**, you can delete any auditor account except the last **Super Auditor**.

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 targets or groups to which they have access.
3. Select the users you want to delete, and then click **Delete**.

> **See Also:**
>
> Logging in to the Audit Vault Server Console

4.2 Creating Templates and Distribution Lists for Email Notifications

Email templates and notifications help auditors to notify other users automatically about audit-related events.

4.2.1 About Email Notifications and Templates

You can configure Oracle Audit Vault and Database Firewall 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.

4.2.2 Creating or Modifying an Email Distribution List

You can create an email distribution list for specific notification purposes, 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.

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

   > **Note:**
   >
   > - An *auditor* can create, modify, and delete email distribution lists that were initially created by the same *auditor*. This is applicable in case of upgrade to Oracle Audit Vault and Database Firewall `12.2.0.8.0` and later.
   > - Email distribution lists that were created prior to upgrade of Oracle Audit Vault and Database Firewall `12.2.0.8.0`, can be modified or deleted by a *super auditor*.

2. Select the **Settings** tab.
3. From the left navigation menu, click **Distribution Lists**.

   The **Distribution Lists** page displays 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.
   - **To** - Enter the email addresses, separated by commas, that appear on the **To** line of notifications using this list.

     > **Note:**
     >
     > Starting in Oracle AVDF 20.11, the **To** and **CC** fields are combined into the required **Email addresses** field. Enter the email addresses, separated by a comma or semicolon, to be added to the list.

   - **CC** - (Optional) Enter the email addresses, separated by commas, that appear on the **CC** line of notifications using this list.

     > **Note:**
     >
     > Starting in Oracle AVDF 20.11, the **To** and **CC** fields are combined into the required **Email addresses** field. Enter the email addresses, separated by a comma or semicolon, to be added to the list.

   - **Description** - (Optional) Enter a description of this list.
   - **Set as default** - (Optional) Starting in Oracle AVDF 20.11, users can select this box to set this distribution list to be the default list for future email notifications for Alert Policies.

5. Click **Save**.

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

> **See Also:**
>
> Logging in to the Audit Vault Server Console

4.2.3 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.

- Oracle AVDF Release 20.1-20.10
- Oracle AVDF Release 20.11 and later

Oracle AVDF Release 20.1-20.10

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

   > **Note:**
   >
   > - An *auditor* can create, modify, and delete email templates that were initially created by the same *auditor*. This is applicable in case of upgrade to Oracle Audit Vault and Database Firewall `12.2.0.8.0` and later.
   > - Email templates that were created prior to upgrade of Oracle Audit Vault and Database Firewall `12.2.0.8.0`, can be modified or deleted by a *super auditor*.

2. Click the **Settings** tab.
3. From the left navigation menu, 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.
4. Click **Create** to create a new template, or click the name of an existing template to modify it.
5. Specify a **Name**.
6. 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.
7. Enter or select the desired values for **Format** and **Description** for the email template.
8. Use the available tags displayed on the right as building blocks for the **Subject** and **Body** of the email.

The available tags depend on the type of notification. Table 4-1 and Table 4-2 explain the tags in detail.

You can either click the tag name to transfer it to the template, or copy and paste the tag name to appear in either the **Subject** or **Body** of the template.

9. Select the appropriate and available options in the **Event Information** section.
10. Click **Save**.

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

Oracle AVDF Release 20.11 and later

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

    > **Note:**
    >
    > - An *auditor* can create, modify, and delete email templates that were initially created by the same *auditor*. This is applicable in case of upgrade to Oracle Audit Vault and Database Firewall `12.2.0.8.0` and later.
    > - Email templates that were created prior to upgrade of Oracle Audit Vault and Database Firewall `12.2.0.8.0`, can be modified or deleted by a *super auditor*.

2. Click the **Settings** tab.
3. From the left navigation menu, click on **Email Templates**.

    The **Email Templates** page displays two sections: a list of pre-defined email templates and a list of user-defined email templates. Users can copy a pre-defined email template to the user-defined email template section. Then, modify the email template as desired. A pre-defined email template will be set as the default until the user defines any user-defined email templates and sets it as the default.

4. To enable the **Copy** button, select a single template by checking the checkbox. Once a single template is selected, the **Copy** button will be clickable.
5. Click **Copy** to create a new user-defined template based on the selected pre-defined one, or click the name of an existing template to view its contents.
6. The copied template will be named "Copy of [Original Template Name]." Edit the **Name** as desired.
7. The **Type** of the copied template will be automatically set based on the original template. Below are the template **Types**:
    - **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.
8. Optionally, add a **Description** for the new user-defined email template.
9. Optionally, click **Set as default** if you would like the newly created template to be your default email template.

10. Click **Copy**.

    After you create a new template, it is listed in the **User-defined email templates** section of the **Email Templates** page.

    From there, you can click the name of the template to modify its details. This includes modifying the above information as well as the following:

    a. You can modify the **Format** of the template to either be Plain Text or HTML.

    b. When your cursor is within the **Body** field, use the available tags displayed on the right as building blocks for the **Body** of the email.

       The available tags depend on the type of notification. Table 4-1 and Table 4-2 explain the tags in detail.

       You can either click the tag name to transfer it to the template, or copy and paste the tag name to appear in the **Body** of the template.

    c. Select the appropriate and available options in the **Event Information** section.

    Additionally, if you click the checkbox for a user-defined email template, the **Copy**, **Delete**, and **Set as default** buttons become clickable.

Table 4-1 lists the available tags for alert notification templates.

Table 4-1 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
`#URL#`	URL of the alert

Table 4-2 lists the available tags for report notification templates.

Table 4-2 Tags Available for Report Attachment or 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"

> **See Also:**
>
> Logging in to the Audit Vault Server Console

4.3 Creating Alert Syslog Templates

Oracle Audit Vault and Database Firewall provides a default template for Oracle Audit Vault and Database Firewall alerts sent to syslog.

If you do not want to use the default template, you can create your own alert syslog templates, and select one to use as a default instead. Using your own template lets you add more information to alert syslog messages.

1. Log in to the Audit Vault Server console as an *auditor*.
2. Click **Settings** tab, and then click **Alert Syslog Templates** in the left navigation menu.
3. In the **Alert Syslog Templates** page, click **Create**.
4. In the **Create Alert Syslog Template** page, enter a **Name** for the new template, and optionally enter the **Description**.
5. Select the **Event Information** that you want to include in syslog alerts from Oracle Audit Vault and Database Firewall.

   The alert syslog message will be formatted as a list of event records containing all fields you select in the template. The short event name (shown in parentheses) will be used.

   If you select **Include "Error Message (EM)" as part of the syslog payload**, then this option lengthens the syslog message so that some data may be truncated.
6. If you want to make this the default template, then select **Save as default template** under **Other options**.

   The default alert syslog template is used for all Oracle Audit Vault and Database Firewall alert syslog messages.
7. Click **Save**.

> **See Also:**
>
> Logging in to the Audit Vault Server Console

4.4 Viewing Monitoring Point and Audit Trail Status

You can view a listing of either the monitoring point status or the audit trail status.

4.4.1 Viewing Monitoring Point Status

Any auditor can view the Database Firewall monitoring points that have been configured for all the target databases.

1. Log into the Audit Vault Server console as an *auditor*.
2. Click **Targets** tab.

3. Click **Database Firewall Monitoring** tab in the left navigation menu.

   This page lists all of the targets, Database Firewall instances, and the status.

4. The current status of the monitoring point is listed in the **Database Firewall Monitoring Status** column.

> **See Also:**
>
> - Working with Lists of Objects in the UI to adjust the appearance of the list from the **Actions** menu.
> - Logging in to the Audit Vault Server Console

4.4.2 Viewing Audit Trail Status

Any auditor can view a list of all audit trails collected for the targets.

1. Log into the Audit Vault Server console as an *auditor*.
2. Click **Targets** tab.
3. Click **Audit Trails** tab in the left navigation menu.

   This page lists all the audit trails for all the targets in a table with the collection status.

4. Optionally, click a column title to sort by the available options.

> **See Also:**
>
> - Working with Lists of Objects in the UI to adjust the appearance of the list from the **Actions** menu.
> - Logging in to the Audit Vault Server Console

4.5 Monitoring Jobs

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

1. Log in to the Audit Vault Server as an auditor.
2. Click on **Settings** tab.
3. Click **Jobs** tab in the left navigation menu.

   A list of jobs is displayed, showing the job type, status, timestamp, and associated user name. To see details for an individual job, click the icon to the left of the specific job.

> **See Also:**
>
> Logging in to the Audit Vault Server Console

5 Managing Global Sets/Data Discovery

Oracle AVDF 20.9 introduced Data Discovery which allowed the creation of global Privileged User and Sensitive Object sets on Oracle Database targets. In Oracle AVDF 20.10 this functionality was renamed to Global Sets and expanded to additionally allow the creation of global IP Address, OS User, Client Program, and Database User sets.

Global sets can be used in multiple Database Firewall Policies at once and simplify the creation of policies.

Global sets should be used when:

- The elements in the set will be used in more than one Database Firewall policy

Local sets should be used when:

- The sets will be used in only one Database Firewall policy
- You want the set to be deleted if the policy gets deleted, such as for a test Database Firewall policy

5.1 Global Sets - Oracle AVDF 20.10 and later

Starting in Oracle AVDF 20.10, Global Sets allows you to create global IP Address, OS User, Client Program, and Database User sets on any type of target database. In addition you can create global Privileged User and Sensitive Objects sets on Oracle Database targets.

5.1.1 About Global Sets

Starting in Oracle AVDF 20.10, Global Sets allows you to create global IP Address, OS User, Client Program, and Database User sets on any type of target database. In addition you can create global Privileged User and Sensitive Objects sets on Oracle Database targets.

Global Sets allows you to add or import IP Addresses, OS user names, client program names, and database user names into sets.

In addition, Global Sets applies User Entitlements and the Database Security Assessment Tool (DBSAT) on your Oracle Database to identify privileged users and sensitive objects. This is enabled by running and scheduling the User Entitlements and Sensitive Object discovery jobs. Once the privileged users and sensitive objects have been discovered, they can be added to privileged user and sensitive objects sets, respectively.

These sets are global and can be used in multiple database firewall policies. Global sets that are created in Global Sets can be viewed in the corresponding tabs in the Database Firewall Policy editor.

Related Topics

- Retrieving User Entitlement Data for Oracle Database Targets
  To retrieve data for user entitlement snapshots, submit or schedule a user entitlement retrieval job for an Oracle Database target.

- Retrieving Sensitive Objects for Oracle Database Targets
  To identify privileged users and sensitive data for data discovery, submit or schedule the sensitive data retrieval job for an Oracle Database target.
- Preparing Targets for Global Sets
- Filtering by a Global Set in an All Activity Report

5.1.2 Prerequisites for Creating Global Privileged User and Sensitive Object Sets

Before global privileged user and sensitive object sets can be created, an `administrator` must enable the permissions on the Oracle Database to run the discovery and user entitlement jobs and the jobs must be initiated and scheduled.

- An `administrator` must enable user privileges for and run statistics gathering on the target Oracle Database. See Preparing Targets for Data Discovery in the *Oracle AVDF Administrator's Guide* for more information.
- The user entitlements retrieval job needs to be initiated and scheduled. See Retrieving User Entitlement Data for Oracle Database Targets for more information.
- The sensitive objects retrieval job needs to be initiated and scheduled. See Retrieving Sensitive Objects for Oracle Database Targets for more information.
- You must be an `auditor` or `super auditor` to use Global Sets (previously called Data Discovery in Oracle AVDF 20.9)

5.1.3 Creating a Global Set

Creating a global set and adding elements to it allows you create one set that can be used in several Database Firewall Policies. IP Address, OS User, Client Program, and Database User sets can be using on any type of target database.

To add elements to a global set:

1. Click **Global Sets** tab.
2. Expand one of the desired IP Address, OS User, Client Program, or Database User sections and click **Add**.
3. Enter a name for the global set.
4. Optionally, enter a description for the global set.
5. Elements can be added to global sets in one or more of the following three ways, From Collected Data, Enter Values, or File Import.
   - **From Collected Data** - Allows you to select specific elements from your targets.
     a. Select one or more targets in the **Available** column and move them to the **Selected** column using the arrows. You can also search for targets as well.
     b. Select if you want to view data from the last 24 hours, week, month, or a specific time period.
     c. Click the **Search** button.
     d. Select the element(s) you would like added to the global set.
   - **Enter Values** - Allows you to type multiple items at once so that the elements can be added in bulk to the global set. Elements can be entered as a comma separated list or one element per line. It is also possible to use both separation methods.

- **File Import** - Allows you to upload a .txt file to add elements to a global set at once. The file can contain elements as a comma separated list or one element per line. It is also possible to use both separation methods.

> **Note:**
>
> If you're importing a file, it must be encoded in the UTF-8 format.

6. Click **Save** once you have added elements to the global set.

5.1.4 Creating Privileged User Sets

Privileged users are identified on your target Oracle Databases through User Entitlements.

1. Click the **Global Sets** tab.
2. Expand the Privileged User Set section and click **Add**.
3. Enter a name for the global set.
4. Optionally, enter a description for the global set.
5. Select one or more targets in the **Available** column and move them to the **Selected** column using the arrows. You can also search for targets as well.
6. Select all the users you'd like to add to the set. Users can be searched for as well.
7. Click **Add**.
8. Click **Save**.

Related Topics

- Managing Privileges for Discovering Privileged Users
- Retrieving User Entitlement Data for Oracle Database Targets

5.1.5 Creating Sensitive Object Global Sets

Sensitive objects are identified on your target Oracle Databases through Database Security Assessment Tool (DBSAT) integration.

1. Click the **Global Sets** tab.
2. Expand the Privileged User Set section and click **Add**.
3. Enter a name for the global set.
4. Optionally, enter a description for the global set.
5. Select one or more targets in the **Available** column and move them to the **Selected** column using the arrows. You can also search for targets as well.
6. Select categories. By default some of the sensitive categories are listed in the selected column and can be removed using the filters.
   Sensitive categories and types available for selection include:
   - **Identification Information:** Includes sensitive types for national, personal, and public identifiers. Examples are US Social Security Number (SSN), Canadian Social Insurance Number (SIN) and other national IDs, Visa Number, and Full Name.

- **Biographic Information:** Includes sensitive types for address, family data, extended PII, and restricted processing data. Examples are Full Address, Mother's Maiden Name, Date of Birth, and Religion.
- **IT Information:** Includes sensitive types for user IT data and device data. Examples are User ID, password, and IP Address.
- **Financial Information:** Includes sensitive types for payment card data and bank account data. Examples are Card Number, Card Security PIN, and Bank Account Number.
- **Healthcare Information:** Includes sensitive types for health insurance data, healthcare provider data, and medical data. Examples include Health Insurance Number, Healthcare Provider, and Blood Type.
- **Employment Information:** Includes sensitive types for employee basic data, organization data, and compensation data. Examples are Job Title, Termination Date, Income, and Stock.
- **Academic Information:** Includes sensitive types for student basic data, institution data, and performance data. Examples are Financial Aid, College Name, Grade, and Disciplinary Record.

7. Select all the users you'd like to add to the set. Users can be searched for as well.
8. Click **Add**.
9. Click **Save**.

Related Topics

- Managing Statistics Gathering for Discovering Sensitive Objects
- Retrieving Sensitive Objects for Oracle Database Targets

5.1.6 Viewing Where Global Sets Are Used

Global Sets allows you to see where global sets are used. This can help identify what policies will be affected if a Global Set is modified.

1. Log in to the Audit Vault Server Console as an `auditor`.
2. Click on the **Global Sets** tab.
3. Click on the name of a global set.
4. View the **Used In** table to determine where the selected global set is used.

Related Topics

- Understanding the Impact of Modifying Global Sets
  When global sets are modified, policies that use the global set will need to be deployed again.

5.1.7 Modifying Global Sets

Modifying elements in a global set allows you to retain the global set while still being able to add or remove elements to or from the set. Modifying a global set makes it easier to update your Database Firewall Policies based on changes to your targets or specific needs, without having to create new sets.

Adding Elements

Elements can be added to all existing sets manually or in bulk for IP Address, OS User, Client Program, and Database User sets.

1. Click **Global Sets** tab.
2. Expand one of the sections and click on an existing global set.
3. For IP Address, OS User, Client Program, and Database User sets you can either click **Add**, **Add From File**, or **Add From Collected Data**. For Privileged User or Sensitive Object sets you can only click **Add.**
4. If you clicked **Add**, in the field that appears type the element(s) you would like to add. Elements can be entered as a comma separated list or one element per line.
5. If you clicked **Add From File** or **Add From Collected Data** the process is the same as when creating a new global set.

> **Note:**
>
> If you're importing a file, it must be encoded in the UTF-8 format.

6. Click **Save**.

Deleting Elements

Elements can be removed from all existing sets manually.

1. Click **Global Sets** tab.
2. Expand one of the sections and click on an existing global set.
3. Select one or more elements from the list that you would like to remove from the global set. You can also search for specific elements as well.
4. Click **Delete**.
5. Click **Save**.

5.1.8 Understanding the Impact of Modifying Global Sets

When global sets are modified, policies that use the global set will need to be deployed again.

From the Global Sets page you can see which of your global sets are currently in use and where they are used. Whenever any set that is in use is modified, i.e. elements are added or removed from it, you will see a dialog box of policies that use the set. These policies will automatically go into a status of **Deployment Required**. Multiple policies in this state can be selected and deployed from the Database Firewall Policies or Alert Policies sections of Oracle AVDF. Deploying these policies will automatically deploy them to any targets the policies were previously deployed on.

While a database firewall policy is in a **Deployment Required** status after a set it uses has been modified, AVDF will continue to use the last deployed version of a policy until the modifications are deployed.

For example, consider the following scenario. There is a global set called AllowedUsers that consists of UserA and UserB which is currently in use by deployed database firewall policy, Policy1. If the AllowedUsers set is modified to additionally include UserC, Policy1 will go into a **Deployment Required** status. Until Policy1 is deployed again the database firewall will only allow traffic from UserA and UserB. Once Policy1 is deployed again then the database firewall will allow traffic from UserA, UserB, and UserC.

> **Note:**
>
> Policies will go into the **Deployment Required** status if any modification occurs to a set, even if that modification is undone. For example, if you add an element to a set, but then remove that element shortly after so that the set includes only the same elements as it did previously, any policies that use the set will still be marked with **Deployment Required**.

5.2 Data Discovery - Oracle AVDF 20.9

In Oracle AVDF 20.9 you can use Data Discovery with your Oracle Databases to create global privileged user and sensitive object sets that can be used in multiple database firewall policies.

5.2.1 About Data Discovery

In Oracle AVDF 20.9 you can use Data Discovery with your Oracle Databases to create global privileged user and sensitive object sets that can be used in multiple database firewall policies.

Data Discovery applies User Entitlements and the Database Security Assessment Tool (DBSAT) on your Oracle Database to identify privileged users and sensitive objects. This is enabled by running and scheduling the User Entitlements and Sensitive Object discovery jobs. Once the privileged users and sensitive objects have been discovered, they can be added to privileged user and sensitive objects sets, respectively. These sets are global and can be used in multiple database firewall policies.

Privileged User and Sensitive Object sets that are created in Data Discovery can be viewed in Data Discovery or in the Database User Sets and Database Objects Sets tabs in the Database Firewall Policy editor. Data Discovery can also be used to create database firewall policies and view and edit policies that were created in Data Discovery.

Related Topics

- Retrieving User Entitlement Data for Oracle Database Targets
  To retrieve data for user entitlement snapshots, submit or schedule a user entitlement retrieval job for an Oracle Database target.
- Retrieving Sensitive Objects for Oracle Database Targets
  To identify privileged users and sensitive data for data discovery, submit or schedule the sensitive data retrieval job for an Oracle Database target.
- Preparing Targets for Data Discovery

5.2.2 Prerequisites for Creating Global Privileged User and Sensitive Object Sets

Before global privileged user and sensitive object sets can be created, an `administrator` must enable the permissions on the Oracle Database to run the discovery and user entitlement jobs and the jobs must be initiated and scheduled.

- An `administrator` must enable user privileges for and run statistics gathering on the target Oracle Database. See Preparing Targets for Data Discovery in the *Oracle AVDF Administrator's Guide* for more information.
- The user entitlements retrieval job needs to be initiated and scheduled. See Retrieving User Entitlement Data for Oracle Database Targets for more information.

- The sensitive objects retrieval job needs to be initiated and scheduled. See Retrieving Sensitive Objects for Oracle Database Targets for more information.
- You must be an `auditor` or `super auditor` to use Global Sets (previously called Data Discovery in Oracle AVDF 20.9)

5.2.3 Creating Privileged User Global Sets

Privileged users are identified on your target Oracle Databases through User Entitlements.

To create a Privileged User Set,

1. Click the **Policies** tab.
2. Click the **Data Discovery** in the left navigation menu.
3. In the Privileged User Sets section, click **Add**.
4. Fill in the set name.
5. Select targets.
6. Select users from the list of **Privileged Users**. To add a new user which is not part of the list, click on the **Add** button and type the name of the user.
7. Click **Save** once done.

5.2.4 Creating Sensitive Object Global Sets

Sensitive objects are identified on your target Oracle Databases through Database Security Assessment Tool (DBSAT) integration.

To create a Sensitive Object set,

1. Click the **Policies** tab.
2. Click **Data Discovery** in the left navigation menu.
3. In the Sensitive Objects Set section click **Add**.
4. Fill in the set name.
5. Select targets.
6. Select categories. By default some of the sensitive categories are listed in the selected column and can be removed using the filters.
   Sensitive categories and types available for selection include:
   - **Identification Information:** Includes sensitive types for national, personal, and public identifiers. Examples are US Social Security Number (SSN), Canadian Social Insurance Number (SIN) and other national IDs, Visa Number, and Full Name.
   - **Biographic Information:** Includes sensitive types for address, family data, extended PII, and restricted processing data. Examples are Full Address, Mother's Maiden Name, Date of Birth, and Religion.
   - **IT Information:** Includes sensitive types for user IT data and device data. Examples are User ID, password, and IP Address.
   - **Financial Information:** Includes sensitive types for payment card data and bank account data. Examples are Card Number, Card Security PIN, and Bank Account Number.

- **Healthcare Information:** Includes sensitive types for health insurance data, healthcare provider data, and medical data. Examples include Health Insurance Number, Healthcare Provider, and Blood Type.
- **Employment Information:** Includes sensitive types for employee basic data, organization data, and compensation data. Examples are Job Title, Termination Date, Income, and Stock.
- **Academic Information:** Includes sensitive types for student basic data, institution data, and performance data. Examples are Financial Aid, College Name, Grade, and Disciplinary Record.

7. Select objects from the list of **Sensitive Objects**. To add a new sensitive object which is not part of the list, click on the **Add** button and type the name of the sensitive object.
8. Click **Save** once done.

5.2.5 Viewing Global Sets

Privileged User and Sensitive Object Sets created in Data Discovery are global and can be used in multiple policies. You can view these lists in Data Discovery.

To view a set,

1. Click the **Policies** tab.
2. Click **Data Discovery** in the left navigation menu.
3. Click on the set name in the corresponding set section in Data Discovery. You will see the list of all privileged users or sensitive objects included in this set. You can use the **Actions** menu to filter the set.

Privileged user sets and sensitive object sets can also be viewed in the **Database User Sets** and **Database Object Sets** tabs in the **Sets/Profiles** of a database firewall policy, respectively.

> **Note:**
>
> Sets can't be edited. You need to delete and create a new set if you would like to make adjustments to an existing set.

Related Topics

- Creating And Managing Database Firewall Sets and Profiles
  Learn how an auditor creates and manages Database Firewall sets and profiles.
- Editing a Database Firewall Policy
  Learn how to edit a Database Firewall policy.

5.2.6 Creating Database Firewall Policies from Data Discovery

Database firewall policies that will use existing Privileged User and Sensitive Object Sets can be created from the Data Discovery section.

To create a database firewall policy,

1. Click the **Policies** tab.
2. Click **Data Discovery** in the left navigation menu.
3. In the Database Firewall Policies section, click **Add**.

4. Fill in the policy name.
5. Select targets.
6. Select the privileged user sets.
7. Select sensitive object sets.
8. Select the statement classes and chose the action to be taken.
9. Click **Save** once done.

Once complete a new policy will be created and will consist of the following:

- DB User Set - created if a privileged user sets was created
- Profile - created if you selected any privileged users for the policy
- Session Context Rule - created if you only selected privileged users for the policy
- Database Object Rule - created if you selected sensitive tables or statement classes. The rule will apply the profile if the profile was created.

The profile can be viewed in the workflow to edit a database firewall policy.

5.2.7 Viewing and Editing Database Firewall Policies

Database firewall policies that were created in Data Discovery can be viewed in the Data Discovery section or the Database Firewall Policies section.

To view database firewall policies that were created in Data Discovery,

1. Click the **Policies** tab.
2. click **Data Discovery** or **Database Firewall Policies** in the left navigation menu.

Policies that use global sets but were created using the standard policy creation workflow in the **Database Firewall Policies** section will not be listed on the Data Discovery page.

In the **Database Firewall Policies** section, policies that were created in Data Discovery will not be designated differently but will appear in the list of User-defined Database Firewall Policies.

To edit a database firewall policy, click the policy name and see Editing a Database Firewall Policy.

6 Creating Audit Policies for Oracle Databases

You can retrieve and provision audit configurations for an Oracle Database.

6.1 About Audit Policies

Using the Audit Vault Server console, you can retrieve audit policies from Oracle Database 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.

- Unified audit policies
- SQL statements
- Schema objects
- Privileges
- Fine-grained auditing

6.2 General Steps for Creating Audit Policies for Oracle Databases

To create audit policies for Oracle databases, you retrieve the target Oracle Database audit policy settings, modify them, and provision the policy.

The general steps that you follow are:

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

6.3 Retrieving and Modifying Audit Policies from an Oracle Database

You can retrieve audit policies from Oracle database.

6.3.1 Understanding the Columns on the Audit Policies Tab

When you retrieve audit policies from a target Oracle Database, you see the state of the database audit policies at that point in time.

Click the **Policies** tab in the Audit Vault Server console. The **Audit Policies** tab in the left navigation menu is displayed by default. This page contains a list of Oracle Database targets. It also lists the time at which the audit policies were last provisioned and retrieved.

Table 6-1 describes the columns shown in the Audit Policies page.

Table 6-1 Fields under Audit Policies tab

Column	Description
Target	Name of the target.
Last Retrieved	The time that the audit information for the selected database was last retrieved.
Last Provisioned	The time that the audit settings were last provisioned to the database from Oracle Audit Vault and Database Firewall.

6.3.2 Retrieving Audit Policies from Multiple Oracle Databases

You can retrieve audit policies from several Oracle Database targets at once. You can schedule audit setting retrievals for individual targets.

After patching to Oracle AVDF 20.12, you will need to

1. Rerun the Oracle privileges script for successful audit policy retrieval for container database targets. For more information see Oracle Database Setup Scripts.
2. Retrieve audit policies before provisioning or viewing audit policies. For more information see Retrieving and Modifying Audit Policies from an Oracle Database

Prerequisite:

- Ensure the target user has sufficient privileges granted for audit policy management. An administrator can grant these using the Oracle Database Setup Scripts.

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

   This page lists a summary of audit policies at this point in time for all targets with their status.
3. In the **Target** column, select the check boxes for the target databases that you want to retrieve audit policies. You can only see the Oracle database targets to which you have access.

> **Note:**
>
> - Traditional auditing is supported for all versions of Oracle Database supported by Oracle AVDF 20 except for Oracle Database 23ai. Traditional auditing is desupported in Oracle Database 23ai. Oracle recommends that you use unified auditing. However, if you upgrade an existing Oracle Database registered with Oracle AVDF to 23ai, any existing traditional audit policies will continue to work, but creating new or enabling previously disabled traditional audit policies is not allowed. For more information see Handling the Desupport of Traditional Auditing in the *Oracle Database Security Guide* and Traditional Auditing Desupported in the *Oracle Database Upgrade Guide*.
> - Unified Auditing is supported for Oracle Database versions starting from 12.2.0.1.

4. Click **Retrieve** button.

   To check the status of the retrieval, click the **Settings** tab. Then click on **Jobs** tab in the left navigation menu. When the audit policies retrieval is complete, the `Audit Settings` is displayed on this page under **Job Type** column.

> **See Also:**
>
> - Scheduling the Retrieval of Audit Settings for an Oracle Database
> - Logging in to the Audit Vault Server Console
> - Understanding the Columns on the Audit Policies Tab

6.3.3 Scheduling the Retrieval of Audit Settings for an Oracle Database

To retrieve audit policy settings for an Oracle Database, schedule an audit policy retrieval job for the target.

After patching to Oracle AVDF 20.12, you will need to

1. Rerun the Oracle privileges script for successful audit policy retrieval for container database targets. For more information see Oracle Database Setup Scripts.
2. Retrieve audit policies before provisioning or viewing audit policies. For more information see Retrieving and Modifying Audit Policies from an Oracle Database

1. Log in to the Audit Vault Server console as an auditor.
2. Click the **Targets** tab.
3. Click the **Schedule Retrieval Jobs** icon for the target.
4. On the Schedule Retrieval Jobs page, select one of the following options under **Audit Policy**:
   - To run the job immediately, select **Retrieve Immediately**.
   - To schedule the job or change an existing schedule, follow these steps:
     a. Select **Create/Update Schedule**.

   b. Select **Enable**.
   c. Enter the start date and time and the repetition frequency.
5. Click **Save**.

Related Topics

- Logging in to the Audit Vault Server Console
  To log in to the Audit Vault Server console, you must have a valid user name and password.
- Monitoring Jobs
  You can see the status of Audit Vault Server jobs, such as report generation, and user entitlement, or audit policy retrieval from targets.
- Managing Targets
  You can view and change target settings, create and modify target groups, manage compliance settings, and set access rights to targets and groups.

6.4 Provisioning Unified Audit Policies

Learn about provisioning Unified Audit policies.

After patching to Oracle AVDF 20.12, you will need to

1. Rerun the Oracle privileges script for successful audit policy retrieval for container database targets. For more information see Oracle Database Setup Scripts.
2. Retrieve audit policies before provisioning or viewing audit policies. For more information see Retrieving and Modifying Audit Policies from an Oracle Database

6.4.1 Basic Auditing

Learn about basic auditing. It captures logon events, critical activity and schema changes.

The basic audit policy **Critical Database Activity** is defined as follows and is enabled for all the database users.

```
CREATE AUDIT POLICY ORA_AV$_CRITICAL_DB_ACTIVITY
PRIVILEGES EXEMPT ACCESS POLICY,EXEMPT REDACTION POLICY,
    ADMINISTER KEY MANAGEMENT,EXPORT FULL DATABASE,IMPORT FULL DATABASE,
    CREATE PUBLIC DATABASE LINK, ALTER PUBLIC DATABASE LINK, DROP PUBLIC
DATABASE LINK,
    CREATE PUBLIC SYNONYM, DROP PUBLIC SYNONYM,
    SELECT ANY DICTIONARY, ADMINISTER DATABASE TRIGGER,
    PURGE DBA_RECYCLEBIN, LOGMINING
ACTIONS CREATE USER, ALTER USER, DROP USER,
        CREATE ROLE, DROP ROLE, ALTER ROLE, SET ROLE, GRANT, REVOKE,
        CREATE PROFILE, ALTER PROFILE, DROP PROFILE,
        CREATE PLUGGABLE DATABASE, DROP PLUGGABLE DATABASE, ALTER PLUGGABLE
DATABASE,
        CREATE LOCKDOWN PROFILE, ALTER LOCKDOWN PROFILE, DROP LOCKDOWN
PROFILE,
        ALTER DATABASE, ALTER SYSTEM,
        CREATE TABLESPACE, ALTER TABLESPACE, DROP TABLESPACE,
        CREATE ROLLBACK SEGMENT, ALTER ROLLBACK SEGMENT, DROP ROLLBACK
SEGMENT,
        CREATE DIRECTORY, DROP DIRECTORY,
        CREATE DISK GROUP,ALTER DISK GROUP,DROP DISK GROUP,
        CREATE PFILE,CREATE SPFILE
ACTIONS COMPONENT = datapump EXPORT,IMPORT
ACTIONS COMPONENT = DIRECT_LOAD LOAD;

AUDIT POLICY ORA_AV$_CRITICAL_DB_ACTIVITY;
-- enabled for all users
```

The basic audit policy **Logon/Logoff Events** audits logon and logoff activities for database users except for a specified list of users and audits all unsuccessful logons and logoffs.

The following policies are provisioned on the target database for logon events category:

```
CREATE AUDIT POLICY ORA_AV$_LOGON_EVENTS ACTIONS LOGON,LOGOFF;
CREATE AUDIT POLICY ORA_AV$_LOGON_FAILURE ACTIONS LOGON,LOGOFF;

AUDIT POLICY ORA_AV$_LOGON_EVENTS EXCEPT <comma separated user list>;
AUDIT POLICY ORA_AVS$_LOGON_FAILURE whenever not successful;
```

The basic audit policy **Database Schema** is defined as follows and is enabled for all the database users.

```
CREATE AUDIT POLICY ORA_AV$_DB_SCHEMA_CHANGES
PRIVILEGES
        CREATE EXTERNAL JOB, CREATE JOB, CREATE ANY JOB
ACTIONS CREATE PROCEDURE, DROP PROCEDURE, ALTER PROCEDURE,
        CREATE PACKAGE, ALTER PACKAGE, DROP PACKAGE, CREATE PACKAGE BODY,
ALTER PACKAGE BODY, DROP PACKAGE BODY,
        CREATE FUNCTION, DROP FUNCTION, ALTER FUNCTION,
        CREATE TRIGGER, ALTER TRIGGER, DROP TRIGGER,
        CREATE LIBRARY, ALTER LIBRARY, DROP LIBRARY,
        CREATE SYNONYM, DROP SYNONYM,
        CREATE TABLE, ALTER TABLE, DROP TABLE, TRUNCATE TABLE,
        CREATE DATABASE LINK, ALTER DATABASE LINK, DROP DATABASE LINK,
        CREATE INDEX, ALTER INDEX, DROP INDEX,
        CREATE OUTLINE, ALTER OUTLINE,DROP OUTLINE,
        CREATE CONTEXT, DROP CONTEXT,
        CREATE ATTRIBUTE DIMENSION,ALTER ATTRIBUTE DIMENSION,DROP ATTRIBUTE
DIMENSION,
        CREATE DIMENSION,ALTER DIMENSION,DROP DIMENSION,
        CREATE INDEXTYPE,ALTER INDEXTYPE,DROP INDEXTYPE,
        CREATE OPERATOR,ALTER OPERATOR,DROP OPERATOR,
        CREATE JAVA,ALTER JAVA,DROP JAVA,
        CREATE MINING MODEL,ALTER MINING MODEL,DROP MINING MODEL,
        CREATE TYPE BODY,ALTER TYPE BODY,DROP TYPE BODY,
        CREATE TYPE,ALTER TYPE,DROP TYPE,
        CREATE MATERIALIZED VIEW,ALTER MATERIALIZED VIEW,DROP MATERIALIZED
VIEW ,
        CREATE MATERIALIZED VIEW LOG, ALTER MATERIALIZED VIEW LOG,DROP
MATERIALIZED VIEW LOG,
        CREATE MATERIALIZED ZONEMAP, ALTER MATERIALIZED ZONEMAP,DROP
MATERIALIZED ZONEMAP,
        CREATE VIEW, ALTER VIEW, DROP VIEW,CREATE ANALYTIC VIEW, ALTER
ANALYTIC VIEW, DROP ANALYTIC VIEW,
        CREATE SEQUENCE, ALTER SEQUENCE, DROP SEQUENCE,
        CREATE CLUSTER, ALTER CLUSTER, DROP CLUSTER,TRUNCATE CLUSTER;

AUDIT POLICY ORA_AV$_DB_SCHEMA_CHANGES;
-- enabled for all users
```

6.4.2 Admin Activity Auditing Policy

Learn about provisioning the Admin Activity Auditing policy.

The Admin Activity Auditing policy lets you audit all activities by privileged administrators. These administrators can make significant changes to the wider system. A database administrator (DBA) can have access to sensitive data that is not protected by realms, and can exfiltrate. The Admin Activity auditing policy audits all activities for non Oracle maintained user who has one of the following privileges or roles.

- **Admin privileges:**

  SYSOPER, SYSDG, SYSKM, SYSRAC, and SYSBACKUP

- **Roles:**

  DBA, DATAPUMP_EXP_FULL_DATABASE, DATAPUMP_IMP_FULL_DATABASE, EXP_FULL_DATABASE, IMP_FULL_DATABASE

Note:

- Non Oracle maintained users are subset of users from dba_users group with oracle_maintained flag set to N.
- Oracle maintained users are subset of users from dba_users group with oracle_maintained flag set to Y.
- See My Oracle Support to download and apply the RDBMS patch 21493004 on the target Oracle Database. Apply the patch to audit only top level statements with unified auditing. This patch must be applied on Oracle Database targets (version 12.2). Also apply the patch on Oracle Database targets (versions prior to 18c). In case this patch is not applied, the following error message is observed in the Audit Vault Server console when All Admin Activity policy is attempted for provisioning:

  ```
  Unable to provision All Admin Activity audit policy on the target
  database. Refer to Admin Activity Audit Policy section in Auditor's
  Guide for details.
  ```

  Instructions for finding patches on My Oracle Support: How to find a patch on My Oracle Support

The following audit policy gets provisioned on the target database (version 12.2.0.1 or greater):

```
CREATE AUDIT POLICY ORA_AV$_ADMIN_USER_ACTIVITY ACTIONS ALL
WHEN SYS_CONTEXT('USERENV','CURRENT_USER') NOT IN
(<list of oracle maintained users>) EVALUATE PER STATEMENT
```

```
AUDIT POLICY ORA_AV$_ADMIN_USER_ACTIVITY BY USERS WITH GRANTED ROLES DBA,
DATAPUMP_EXP_FULL_DATABASE, DATAPUMP_IMP_FULL_DATABASE, EXP_FULL_DATABASE,
IMP_FULL_DATABASE;

AUDIT POLICY ORA_AV$_ADMIN_USER_ACTIVITY BY PUBLIC, SYSDG, SYSKM, SYSRAC,
SYSBACKUP;
```

> **Note:**
>
> To get the list of Oracle maintained users, run query:
>
> ```
> SELECT username from dba_users where oracle_maintained = 'Y'
> ```

On Oracle Database 19c and above, the system provisions an additional audit policy to monitor all top level activities of `SYS` as shown here:

```
CREATE AUDIT POLICY ORA_AV$_SYS_TOP_ACTIVITY ACTIONS ALL ONLY TOPLEVEL;
AUDIT POLICY ORA_AV$_SYS_TOP_ACTIVITY by SYS;
```

Starting Oracle AVDF release 20.3, the following audit policy gets provisioned on the target database:

```
CREATE AUDIT POLICY ORA_AV$_ADMIN_USER_ACTIVITY ACTIONS ALL WHEN
SYS_CONTEXT('USERENV','CURRENT_USER') NOT IN(<list of oracle maintained
users>) EVALUATE PER STATEMENT ONLY TOPLEVEL;
```

After upgrading from Oracle AVDF releases 20.1 or 20.2 to 20.3, follow these steps before provisioning unified audit policies. Also apply the patch on Oracle Database targets (versions prior to 18c) to audit only top level statements with unified auditing. See My Oracle Support to download and apply the RDBMS patch 21493004 on the target Oracle Database.

1. Log in to the Audit Vault Server console as *auditor*.
2. Click **Policies** tab.
3. The **Audit Policies** tab in the left navigation menu is selected by default.
4. Click the specific target.
5. The policy details page is displayed. Disable the `Admin User Activity` category.
6. Log in to the target database as the target user and run these commands:

   ```
   DROP AUDIT POLICY ORA_AV$_ADMIN_USER_ACTIVITY;
   ```

   ```
   DROP AUDIT POLICY ORA_AV$_SYS_TOP_ACTIVITY;
   ```

7. Return to the **Audit Policies** sub tab in the Audit Vault Server console.
8. Select the specific policy and click **Retrieve** button in the top right corner.
9. Enable the `Admin User Activity` category.

6.4.3 User Activity Auditing Policy

Learn about provisioning the User Activity Auditing policy.

The User Activity Auditing policy tracks all activity by users who may have access to sensitive data or who are under observation. These users could be “non-admin but privileged” users. When enabling this policy in the interface, you must specify non-Oracle maintained users to audit.

The following audit policy gets provisioned on the target database:

```
CREATE AUDIT POLICY ORA_AV$_USER_ACTIVITY ACTIONS ALL
WHEN SYS_CONTEXT('USERENV','CURRENT_USER') NOT IN
(<list of oracle maintained users>) EVALUATE PER STATEMENT

AUDIT POLICY ORA_AV$_USER_ACTIVITY BY <comma-separated non-Oracle maintained
user list>
```

6.4.4 Audit Compliance Standards

Learn about audit compliance standards supported in Oracle AVDF.

6.4.4.1 Center for Internet Security Recommendations Unified Audit Policy

Learn about provisioning Center for Internet Security Recommendations (CIS) unified audit policy.

The Center for Internet Security Recommendations (CIS) unified audit policy is a predefined policy (`ORA_CIS_RECOMMENDATIONS`) in Oracle Database specifically designed to perform audits that the CIS recommends.

You can enable or disable this policy, along with other policies provided by Oracle Audit Vault and Database Firewall. This policy tracks many activities and can help you evaluate whether you are adhering to database compliance requirements. For example, you can track when a user, database link, profile, or procedure is created, altered, or dropped.

CIS is a world-recognized organization that provides consensus-based best practices for helping organizations assess and improve their cyber security posture. They provide resources, such as configuration assessment tools, secure configuration benchmarks, security metrics, and certifications. One of the main objectives of the organization is to help businesses prioritize what they need to do for security, and they strive to provide recommendations in simple, non-technical terms.

Related Topics

- *Oracle Database Security Guide*

6.4.4.2 Security Technical Implementation Guidelines (STIG)

Learn about enabling Security Technical Implementation Guidelines (STIG) unified audit policy.

Starting Oracle AVDF 20.5, **Security Technical Implementation Guidelines (STIG)** unified audit policy is available for provisioning. This functionality can be enabled on Oracle Database targets to implement Security Technical Implementation Guidelines (STIG) audit requirements.

Security Technical Implementation Guidelines (STIG) can be enabled on Oracle Database targets starting with version 21.

When Security Technical Implementation Guidelines (STIG) is provisioned, the following unified policies are enabled on the target database.

Predefined Audit Policies Name	Can be enabled for users	Event Condition
`ORA_STIG_RECOMMENDATIONS`	All users	• Success • Failure
`ORA_LOGON_LOGOFF`	All users	• Success • Failure
`ORA_ALL_TOPLEVEL_ACTIONS`	Privileged users	• Success • Failure

You can fetch the privileged user list identified by the user entitlement job or provide your own list. You can enable or disable this policy, along with other policies provided by Oracle AVDF. This policy tracks many activities and can help you evaluate whether you are adhering to STIG compliance requirements or not.

Follow these steps to enable STIG audit policy. These options are applicable only for `ORA_ALL_TOPLEVEL_ACTIONS` audit policy.

1. Log in to the Audit Vault Server console as an *auditor*.
2. Click on **Policies** tab. The **Audit Policies** tab in the left navigation menu is selected by default.

   > **Note:**
   >
   > In case the **Last Retrieved** timestamp is greater than two hours, then do an audit retrieval first.

3. Click the name of Oracle Database target for which you want to provision the audit policies.

   Unified Auditing sub tab in the main page is selected by default.
4. Under **Audit Compliance Standards**, click the checkbox against **Security Technical Implementation Guidelines (STIG)** to enable this functionality.
5. In case `ORA_ALL_TOPLEVEL_ACTIONS` under **Oracle Predefined Policies** is already applied for the specific set of users or roles, then a confirmation dialog is displayed with a message.

   ```
   ORA_ALL_TOP_LEVEL_ACTIONS policy is enabled on the target database for
   specific users/roles. Enabling STIG Compliance will override those changes. Do
   you want to continue?
   ```
6. Click on **OK** or **Cancel**. Upon clicking **Cancel**, the checkbox against Security Technical Implementation Guidelines (STIG) will be unchecked and you will not be able to enable STIG.
7. In case the checkbox against **Security Technical Implementation Guidelines (STIG)** is checked, then it can be modified. An edit icon appears next to it. Click on the edit icon. The **Configure STIG** dialog is displayed.
8. You can provide the privileged users for enabling the policy using either or both of the below options:

- **Privileged Users identified by User Entitlements**
- **Include Privileged Users**

> **Note:**
>
> - If you choose **Privileged Users identified by User Entitlements**, then `ORA_ALL_TOPLEVEL_ACTIONS` policy is enabled for all the privileged users identified by the user entitlement job. The **Last Retrieved** timestamp displays the time of the last retrieved user entitlement job. If the last retrieved time is greater than a day, then it is better to perform the user entitlement retrieval again before provisioning the **Security Technical Implementation Guidelines (STIG)** so that you have the latest list of privileged users.
> - If the **Last Retrieved** time is null, then it means that user entitlement was never retrieved. You need to retrieve user entitlement before provisioning **Security Technical Implementation Guidelines (STIG)**. See Retrieving User Entitlement Data for Oracle Database Targets for more information.
> - If you choose **Privileged Users identified by User Entitlements**, then you can automatically apply the STIG policy for latest list of privileged users. Click the checkbox against **Automatically update ORA_ALL_TOPLEVEL_ACTIONS when Privileged Users change**. When this option is selected, whenever a user entitlement job runs and if the privileged users have changed, then the `ORA_ALL_TOPLEVEL_ACTIONS` audit policy is enabled again for the latest list of privileged users. You can schedule the user entitlement job so that STIG is enabled for all privileged users.
> - If you choose **Include Privileged Users** option, then manually enter the list of privileged users.

9. Click **Save**.
10. Click **Provision Unified Policy** button in the top right corner to provision the policy.
11. To check the provisioning status, click the **Settings** tab. Then click on **Jobs** tab in the left navigation menu. When the job is submitted successfully, the `Unified Audit Policy` job is displayed on the page under **Job Type** column.

6.4.5 User-defined and Oracle Pre-defined Unified Policies

Learn about provisioning custom and Oracle pre-seeded unified policies.

You can enable **Oracle Pre-defined Policies** or **User-defined Policies** that you created on your target database using Oracle Audit Vault and Database Firewall. The following are **Oracle Pre-defined Policies**:

Table 6-2 Oracle Pre-defined Policies

Oracle Pre-defined Policy	Oracle Database Version
`ORA_ACCOUNT_MGMT`	All versions
`ORA_ALL_TOPLEVEL_ACTIONS`	Oracle Database 20.1 and later

Table 6-2 (Cont.) Oracle Pre-defined Policies

Oracle Pre-defined Policy	Oracle Database Version
ORA_DATABASE_PARAMETER	All versions
ORA_DV_AUDPOL	All versions Replaced by ORA_DV_SCHEMA_CHANGES in Oracle Database 23ai
ORA_DV_AUDPOL2	Oracle Database 12.2.0.1 and later Replaced by ORA_DV_DEFAULT_PROTECTION in Oracle Database 23ai
ORA_DV_DEFAULT_PROTECTION This replaced ORA_DV_AUDPOL2 from previous versions.	Oracle Database 23ai
ORA_DV_SCHEMA_CHANGES This replaced ORA_DV_AUDPOL from previous versions.	Oracle Database 23ai
ORA_LOGIN_LOGOUT	Oracle Database 23ai
ORA_LOGON_FAILURES	All versions
ORA_LOGON_LOGOFF	Oracle Database 20.1 and later
ORA_OLS_SCHEMA_CHANGES	Oracle Database 23ai
ORA_RAS_POLICY_MGMT	All versions
ORA_RAS_SESSION_MGMT	All versions
ORA_SECURECONFIG	All versions
ORA$DICTIONALY_SENS_COL_ACCESS	Oracle Database 23ai

Tip:

It is recommended to use the newest policy name when upgrading from a previous version of Oracle Database.

Starting Oracle AVDF 20.4, User-defined and Oracle Pre-defined Unified policies can be enforced on users, roles, and on specific event conditions (successful, unsuccessful, or both).

> **Note:**
>
> In case the policies have been enabled or disabled directly from the target database after the last retrieval, then they have to be retrieved again. This is done to fetch the updated list of the unified audit policies that are enabled or disabled on the target database.

Follow these steps to edit the audit policy for users or roles:

1. Log in to the Audit Vault Server console as an *auditor*.
2. Click **Policies** tab. The **Audit Policies** tab in the left navigation menu is selected by default.
3. Click on the name of the specific Oracle Database target for which you want to provision the audit policies.
4. **Unified Auditing** sub tab in the main page is selected by default.
5. If the checkbox against any pre-defined or user-defined policy is checked, then it can be modified. An edit icon appears next to it.
6. Click on the edit icon. The **Configure Policy** dialog is displayed.
7. Based on users, the audit policy can be enabled for:
   - All users
   - Only a specific set of users and/or roles
   - All users except a specific set of users
8. Based on event status, the audit policy can be enabled for:
   - Successful events
   - Unsuccessful events
   - Both successful and unsuccessful events
9. If you choose to modify or enable for only a specific set of users and/or roles, then a table appears. This table has two columns. You can add additional users and event status details. You can also delete any existing entries.
10. If you choose to modify or enable for all users and exclude only a specific set of users, then a table component appears. You can move users from the **Available** column to **Excluded** column to exclude specific users. You can also select the event status (successful, unsuccessful, both) beneath the table.
11. Choose or edit the values according to your specification in the dialog.
12. Click **Save**.
13. Click **Provision Unified Policy** to provision the policy.
14. Check the **Jobs** section for the status.

> **Note:**
>
> To view the list of roles, follow the steps for Retrieving User Entitlement Data for Oracle Database Targets.

6.4.6 Provisioning Unified Audit Policies from the Audit Vault Server

You can provision unified audit policies from the Audit Vault Server to the Oracle Database target.

This updates the audit policies in the target without the intervention of a database administrator. However, a database administrator can modify or delete these audit policies, as well as add new ones. For this reason, you should periodically retrieve the settings to ensure that you have the latest audit policies.

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

   The Audit Settings page is displayed, showing the Oracle database targets to which you have access.
3. Click the name of a target database.
4. Click **Unified Auditing** sub tab on the main page.
5. Select one or more check boxes to enable or disable the policy.
6. Click **Provision Unified Policy** button in the top right corner.

   To check the provisioning status, click the **Settings** tab. Then click on **Jobs** tab in the left navigation menu. When the job is submitted successfully, the `Unified Audit Policy` job is displayed on the page under **Job Type** column.

   > **Note:**
   >
   > Ensure the target user has sufficient privileges granted for audit policy management. This can be accomplished by running Oracle Database Setup Scripts.

   For Unified audit policy retrieval and provisioning for CDBs and PDBs, the audit policies can be provisioned or retrieved by treating every PDB as an independent target. A CDB can be registered for audit policy management. While provisioning a CDB, audit policies can be included for CDB only, or for CDB and all PDBs. In case CDB and all PDBs are selected, it propogates policies for all the PDB instances. Log in to the Audit Vault Server console and click the **Policies** tab. In the left navigation menu, select **Audit Policies**. Under the **Unified Auditing** sub tab and under the **Core Policies** section of the main page, there are two radio buttons at the bottom:

   a. **Container & All Pluggable Databases**

   b. **Container Database Only**

   Choose these options accordingly and complete the audit policy provisioning. Upon successfully provisioning of the audit policies for a CDB target, the buttons are disabled and cannot be selected again.

See Also:

- Retrieving Audit Policies from Multiple Oracle Databases
- Logging in to the Audit Vault Server Console

6.5 Provisioning Traditional Audit Policies

Traditional audit policies are used to monitor SQL statements, schema objects, privileges, and fine-grained auditing.

After patching to Oracle AVDF 20.12, you will need to

1. Rerun the Oracle privileges script for successful audit policy retrieval for container database targets. For more information see Oracle Database Setup Scripts.
2. Retrieve audit policies before provisioning or viewing audit policies. For more information see Retrieving and Modifying Audit Policies from an Oracle Database

Note:

Traditional auditing is desupported in Oracle Database 23ai. Oracle recommends that you use unified auditing. However, if you upgrade an existing Oracle Database registered with Oracle AVDF to 23ai, any existing traditional audit policies will continue to work, but creating new or enabling previously disabled traditional audit policies is not allowed. For more information see Handling the Desupport of Traditional Auditing in the *Oracle Database Security Guide* and Traditional Auditing Desupported in the *Oracle Database Upgrade Guide*.

Related Topics

- Provisioning Unified Audit Policies
  Learn about provisioning Unified Audit policies.

6.5.1 About Creating Audit Policy Settings

After you retrieve audit policy settings from the target Oracle database, and selected the settings you need, you can create new policy settings for the Oracle database.

Caution:

- Any audit setting that is not indicated as **Needed** in the Audit Vault Server console will be turned off on the target. See "Specifying which Audit Policies are needed".
- After you have updated and/or created the audit policies for a target Oracle Database, you can provision the audit policy changes to that database.

6.5.2 Specifying which Audit Policies are needed

After you retrieve the audit policies from the target Oracle Database, you can view and modify them as needed.

Remember that you are modifying audit policies in use at the time you retrieved them. If you think they may have changed, you should retrieve them again.

1. Log in to the Audit Vault Server console as an *auditor*.
2. Click **Policies** tab. The **Audit Policies** tab in the left navigation menu is selected by default.
3. Click on the name of the specific Oracle Database target for which you want to change the audit policies.
4. An overview page for the target displays two sections:
   - **Unified Auditing**
   - **Traditional Auditing**
5. Click **Traditional Auditing**. It displays the audit policies in use and marked as needed for the audit types:
   - Statement
   - Object
   - Privilege
   - FGA
6. Click on the link of the specific audit type to update the settings. For example, **Object**.

   The Object audit policies for the specific target is displayed on the page. This is the current audit policies. The second column displays a problem icon if there is a difference between the setting at the target database, and the setting in Oracle Audit Vault and Database Firewall.
7. Select the check boxes for each audit setting you determine is needed, then click **Set as Needed** button on the top right corner.
8. To remove audit policies, select the check boxes for the ones you want to remove, then click **Set as Not Needed**.
9. To create new audit policies for the audit type, click **Create**.

> **See Also:**
>
> - Provisioning Traditional Audit Policies
> - Retrieving Audit Policies from Multiple Oracle Databases
> - Logging in to the Audit Vault Server Console

6.5.3 Creating Audit Policies for SQL Statements

Auditors can create and manage audit policies for SQL statements.

6.5.3.1 About SQL Statement Auditing

Statement auditing audits SQL statements by type of statement, not by the specific schema objects on which the statement operates.

Statement auditing can be broad or focused (for example, by auditing the activities of all database users or only a select list of users). Typically broad statement auditing audits the use of several types of related actions for each option. These statements are in the following categories:

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

6.5.3.2 Defining SQL Statement Audit Settings

Any auditor can define a SQL statement audit policy.

1. Log in to the Audit Vault Server console as an *auditor*.
2. If necessary, retrieve and update the current audit settings.
3. Click the **Policies** tab. The **Audit Policies** tab in the left navigation menu is selected by default.
4. Click on a specific Oracle Database target.
5. An overview page for the target displays two sections:
   - **Unified Auditing**
   - **Traditional Auditing**
6. Click **Traditional Auditing**. Click **Statement** in the column **Audit Type**.

   The statement audit settings of the specific target is displayed.
7. Click the **Create** button.
8. In this page, define the audit policy as follows:
   - **Audit Actions 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.
     - **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.
   - **Execution Condition** - Choose one of the following:
     - **Both:** Audits both successful and failed statements
     - **On Success:** Audits the statement if it is successful
     - **On 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.

9. Click **Save**.

   The new audit settings are added to the statement audit settings page.

> **See Also:**
>
> - Retrieving and Modifying Audit Policies from an Oracle Database
> - Understanding the Statement Audit Settings
> - Logging in to the Audit Vault Server Console

6.5.3.3 Understanding the Statement Audit Settings

The Statement Audit Settings page shows status information such as whether the statement is audited or if the statement audit policy is active.

Table 6-3 lists the columns used in the Statement page.

Table 6-3 Columns in the Statement Audit Settings

Column	Description
(Left most 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 Audit Vault and Database Firewall, but is not in use in the target database. • The setting is in use at the target database, but is not marked as needed in Oracle Audit Vault and Database Firewall.
Setting	The statement that is audited.
In Use	A green check mark indicates if the setting is active in the target database. A red cross mark indicates if it has not been provisioned or is not active.
Needed	A green check mark indicates if the audit setting is marked as needed in Oracle Audit Vault and Database Firewall. A red cross mark indicates if the audit setting is marked as not needed. If an audit setting that is not in use is set to needed, a green check mark appears after provisioning in the **In Use** column. 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: `ACCESS` or `SESSION`
Execution Condition	The execution condition audited: `SUCCESS`, `FAILURE`, or `BOTH`
Proxy User	The proxy user for the database, if any.

Table 6-3 (Cont.) Columns in the Statement Audit Settings

Column	Description
User	The user to which this setting applies, if any.

6.5.4 Creating Audit Policies for Schema Objects

Auditors can create and manage schema object audit policies.

6.5.4.1 About Schema Object Auditing

Schema object auditing is the auditing of specific statements on a particular schema object, such as `AUDIT SELECT ON HR.EMPLOYEES`.

Schema object auditing is very focused, auditing only a specific statement on a specific schema object for all users of the database.

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

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

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

6.5.4.2 Defining Schema Object Audit Settings

Any auditor can define a schema object audit policy.

1. Log in to the Audit Vault console as an *auditor*.
2. If necessary, retrieve and update the current audit settings.
3. Click **Policies** tab. The **Audit Policies** tab in the left navigation menu is selected by default.
4. Click on a specific target Oracle database.

   An overview page for the target displays two sections:

   - **Unified Auditing**
   - **Traditional Auditing**
5. Click on **Traditional Auditing**.
6. Click **Object** to display the Object Audit Settings of the specific target.
7. Click the **Create** button.
8. 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.
   - **Execution Condition -** Choose one of the following:

  - **Both:** Audits both successful and failed statements
  - **On Success:** Audits the statement if it is successful
  - **On 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.

9. Click **Save**.

   The newly defined object audit settings is added to the Object Audit Settings page.

> **See Also:**
>
> - Logging in to the Audit Vault Server Console
> - Retrieving and Modifying Audit Policies from an Oracle Database
> - Understanding the Object Audit Settings Page for descriptions of the columns used in this page.

6.5.4.3 Understanding the Object Audit Settings Page

The Object Audit Settings page shows object status information such as the object that is being audited and whether the policy is active.

Table 6-4 lists the columns used in the Object page.

Table 6-4 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 Audit Vault and Database Firewall, but is not in use in the target database. • The setting is in use at the target database, but is not marked as needed in Oracle Audit Vault and Database Firewall.
Setting	The statement that is audited
In Use	The arrow points upward if the setting is active in the 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 Audit Vault and Database Firewall, 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.

Table 6-4 (Cont.) Columns in the Object Audit Settings Page

Column	Description
Name	The name of the object in the specified schema.
Type	The object (such as a database table) to which this setting applies
Owner Name	The database schema to which this setting applies
Audit Granularity	The granularity of auditing: `ACCESS` or `SESSION`
Execution Condition	The execution condition audited: `SUCCESS`, `FAILURE`, or `BOTH`

6.5.5 Creating Audit Policies for Privileges

Auditors can create and manage privilege audit policies.

6.5.5.1 About Privilege Auditing

Privilege auditing is the auditing of SQL statements that use a system privilege.

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

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

Privilege auditing audits the use of powerful system privileges enabling corresponding actions, such as `AUDIT CREATE TABLE`. If you set both similar statement and privilege audit options, then only a single audit record is generated. For example, if the statement clause `TABLE` and the system privilege `CREATE TABLE` are both audited, then only a single audit record is generated each time a table is created. The statement auditing clause, `TABLE`, audits `CREATE TABLE`, `ALTER TABLE`, and `DROP TABLE` statements. However, the privilege auditing option, `CREATE TABLE`, audits only `CREATE TABLE` statements, because only the `CREATE TABLE` statement requires the `CREATE TABLE` privilege.

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

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

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

6.5.5.2 Defining Privilege Audit Settings

Any auditor can define a privilege audit policy.

1. Log in to the Audit Vault Server console as an *auditor*.
2. If necessary, retrieve and update the current audit settings.
3. Click **Policies** tab. The **Audit Policies** tab in the left navigation menu is selected by default.

4. Click on the name of the specific Oracle Database target for which you want to change the audit settings.
5. An overview page for the target displays two sections:
   - **Unified Auditing**
   - **Traditional Auditing**
6. Click **Privilege**.

   The Privilege Audit Settings for a specific target is displayed.
7. Click the **Create** button.
8. In the Create Privilege Audit Settings 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 Users** field appears, in which you must specify at least one user. To display a list of proxy users and their 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.
   - **Execution Condition** - Choose one of the following:
     - **Both:** Audits both successful and failed privilege use
     - **On Success:** Audits the privilege use if it is successful
     - **On Failure:** Audits the privilege use 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.
9. Click **Save**.

   The newly defined privilege audit settings is added to the list in the Privilege Audit Settings page.

> **See Also:**
>
> - Understanding the Privilege Audit Settings Page
> - Retrieving and Modifying Audit Policies from an Oracle Database
> - Logging in to the Audit Vault Server Console

6.5.5.3 Understanding the Privilege Audit Settings Page

The Privilege Audit Settings page shows status information such as the privileges being audited and whether an audit policy is active.

Table 6-5 lists the columns used in the Privilege Audit Settings page.

Table 6-5 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 Audit Vault and Database Firewall, but is not in use in the target database. • The setting is in use at the target database, but is not marked as needed in Oracle Audit Vault and Database Firewall.
Setting	The statement that is audited
In Use	The arrow points upward if the setting is active in the 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 Audit Vault and Database Firewall, 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

6.5.6 Creating Audit Policies for Fine-Grained Auditing (FGA)

Auditors can create and manage fine-grained audit policies.

6.5.6.1 About Fine-Grained Auditing

Fine-grained auditing (FGA) enables you to create a policy that defines specific conditions that must exist for the audit to occur.

For example, fine-grained auditing lets you audit the following types of activities:

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

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

6.5.6.2 Using Event Handlers in Fine-Grained Auditing

In a fine-grained audit policy, you can specify an event handler to process an audit event.

The event handler provides flexibility in determining how to handle a triggering audit event. For example, it could write the audit event to a special audit table for further analysis, or it could send a pager or an 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.

6.5.6.3 Auditing Specific Columns and Rows

A fine-grained audit policy 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.

6.5.6.4 Defining Fine-Grained Audit Settings

Any auditor can define a fine-grained audit policy.

1. Log in to the Audit Vault Server console as an *auditor*.
2. If necessary, retrieve and update the current audit settings.
3. Click **Policies** tab. The **Audit Policies** tab in the left navigation menu is selected by default.

4. Click on the name of the specific Oracle Database target for which you want to change the audit settings.

   An overview page for the target displays two sections:

   - **Unified Auditing**
   - **Traditional Auditing**

5. Click on **Traditional Auditing**.
6. Click **FGA**. It displays the Fine Grained Audit Settings page of the specific target.
7. Click the **Create** button.
8. 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:

Definition	Description
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.

   - **Schema** - Select a schema to audit.
   - **Objects** - Select an object to audit.
   - **Statements** - Select one or more SQL statements to be audited. The available options are: `DELETE`, `INSERT`, `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.
   - **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`

- **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`

9. Click **Save**.

   The fine-grained audit policy is created.

> **See Also:**
>
> - Understanding the Fine-Grained Audit Settings Page
> - Retrieving and Modifying Audit Policies from an Oracle Database
> - Logging in to the Audit Vault Server Console
> - Using Event Handlers in Fine-Grained Auditing
> - Auditing Specific Columns and Rows for more information about relevant columns.

6.5.6.5 Understanding the Fine-Grained Audit Settings Page

The Fine-Grained Audit Settings page shows status information, such as the object to which the policy applies.

Table 6-6 lists the columns used in the Fine-Grained Audit Settings page.

Table 6-6   Columns in the Fine-Grained Audit Settings Page

Field	Description
(Leftmost column)	A checkbox for selecting the audit setting
Problem	An exclamation mark icon indicates one of the following conditions: • The setting is marked as needed in Oracle Audit Vault and Database Firewall, but is not in use in the target database. • The setting is in use at the target database, but is not marked as needed in Oracle Audit Vault and Database Firewall.
Name	The name of this fine-grained audit policy
In Use	The arrow points upward if the setting is active in the 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 Audit Vault and Database Firewall, 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 6-6 (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.

6.5.7 Exporting Audit Settings to a SQL Script

You can export audit policy settings for a target to a SQL script from Oracle Audit Vault and Database Firewall.

Then you can give the script to a database administrator for the target Oracle Database to use to update the audit settings on that database.

1. Log in to the Audit Vault console as an *auditor*.
2. Click **Policies** tab. The **Audit Policies** tab in the left navigation menu is selected by default.

   The page displays a list of Oracle Database targets to which you have access.
3. Click the name of the specific Oracle Database target.

   The audit settings overview for the database appears on the page. **Unified Auditing** sub tab is selected by default.
4. Click **Traditional Auditing** sub tab.
5. Select one or more check boxes for the audit types that you want to export: **Statement**, **Object**, **Privilege**, or **FGA**.
6. Click **Export/Provision**.

   The **Export/Provision Audit Settings** page appears. It displays the exportable audit commands.
7. Click the **Export** radio button, then click the **Export** button in the top right corner.
8. Click **OK** to confirm.
9. Save the SQL file to a location on your system.
10. Give the saved script to the database administrator for that target.

    The database administrator can then apply the policies to the target. To verify that the settings have been updated, you can retrieve the audit settings.

> **See Also:**
>
> - Retrieving Audit Policies from Multiple Oracle Databases
> - Logging in to the Audit Vault Server Console

6.5.8 Provisioning Traditional Audit Policies from the Audit Vault Server

You can provision the traditional audit policy settings directly from the Audit Vault Server to the target Oracle Database.

This updates the audit policies in the target without the intervention of a database administrator. However, a database administrator can modify or delete these audit policies, as well as add new ones. For this reason, you should periodically retrieve the settings to ensure that you have the latest audit policies.

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

   The **Audit Policies** tab in the left navigation menu is selected by default. It displays Oracle Database targets to which you have access.
3. Click the name of the specific target database.
4. Click **Traditional Auditing** sub tab on the main page.
5. Select one or more check boxes for the audit types that you want to provision: **Statement**, **Object**, **Privilege**, or **FGA**.
6. Click **Provision Traditional Policy** button.

   The **Export/Provision Audit Settings** page appears. It displays the exportable audit commands, and allowing you to verify them before provisioning. The audit settings can be either exported to a file or provisioned directly to the target.
7. Click the **Provision** radio button below the box.
8. Ensure the target user has sufficient privileges granted for audit policy management using the privilege script.

   > **Note:**
   >
   > Ensure the target user has sufficient privileges granted for audit policy management. This can be accomplished by running Oracle Database Setup Scripts.
9. Click the **Provision** button in the top right corner.
10. Click **OK** to confirm.

    To check the provisioning status, click the **Settings** tab. Then click on **Jobs** tab in the left navigation menu. When the job is submitted successfully, the `Audit Settings` job is displayed on the page under **Job Type** column.

> **See Also:**
>
> - Oracle Database Setup Scripts
> - Retrieving Audit Policies from Multiple Oracle Databases
> - Logging in to the Audit Vault Server Console

6.6 Viewing Unified Audit Policies

Starting in Oracle AVDF 20.12, you can view the audit policies that are enabled on your target databases.

Prerequisites

After patching to Oracle AVDF 20.12, you will need to

1. Rerun the Oracle privileges script for successful audit policy retrieval for container database targets. For more information see Oracle Database Setup Scripts.
2. Retrieve audit policies before provisioning or viewing audit policies. For more information see Retrieving and Modifying Audit Policies from an Oracle Database

Procedure

1. Log in to the Audit Vault Server Console as an `auditor`.
2. Click the **Policies** tab.
3. Select the database(s) you would like to view the audit policies for.
4. Click **View Policies**.
   You will see a table specifying the details of the audit policies for the selected target database(s).

   For a CDB$ROOT target, you can see the list of common policies that have been enabled on the container database (CDB) and the pluggable database(s) (PDB) and the local policies of each individual PDB as well. This will show the policies of all PDBs that have been set up when the audit retrieval was done. If a PDB is added or removed, perform audit retrieval again to see the latest list.

7 Database Firewall Policies

You can create and manage Database Firewall policies.

7.1 About Database Firewall Policies

Database Firewall policies allow you to configure actions that Database Firewall should take on the SQL traffic it is receiving.

Oracle strongly recommends that you read Network-Based SQL Traffic Monitoring with Database Firewall to understand:

- the Database Firewall network placement options
- the different protection modes
- the concepts of how a Database Firewall policy works

Database Firewall policies can be configured to report SQL operations on database, control client application access, enforce expected database access behavior, prevent SQL injection, and control application bypass, and prevent malicious SQL statements from reaching the database.

Database Firewall allows to create an allow list of SQL statements to pass, or deny list to block or alert.

Database Firewall policies is defined based on the users, the actions they can perform on the data, and the actions that the Database Firewall must initiate when the event occurs.

7.2 About Database Firewall Deployment Modes and Policies

Learn about Database Firewall deployment modes and corresponding policy types.

Database Firewall can be deployed in the following modes:

1. **Monitoring (Out-of-Band)**
2. **Monitoring (Host Monitor)**
3. **Monitoring / Blocking (Proxy)**

Monitoring (Out-of-Band) or **Monitoring (Host Monitor)** deployment modes can be used for monitoring only and to alert on potential policy violations.

Monitoring / Blocking (Proxy) mode can be deployed to block certain SQL activities, in addition to monitoring and alerting. For example, policy rule can be defined to block SQL statements that violate the policy guidelines.

Some scenarios to define Database Firewall policies are listed below:

Scenario	Description
Monitoring privileged users	Configure the Database Firewall policy to monitor and capture all the SQL statements run by privileged users. Create a list of privileged users and use this list in **Session Context** rule. This provides all SQL statements run by them over the network for a specific target database. Deploy Database Firewall in any of the three modes and use **Session Context** rule.
Block DBA access to sensitive application database objects	Deploy Database Firewall in **Monitoring / Blocking (Proxy)** mode. Create a list of DBA (Database Administrator) users, configure **Database Object** rule to block any SQL statement run by these users on a list of sensitive objects.
Monitoring sensitive data and access over the network	Configure the Database Firewall policy to monitor user access and their operations on sensitive data by using **Database Object** rule. Provide a list of sensitive objects (table or views) while configuring the **Database Object** rule. Database Firewall can be deployed in any of the three modes in this scenario.
Blocking unauthorized access	Deploy Database Firewall in **Monitoring / Blocking (Proxy)** mode and use the **Database Object** rule. Create a profile of users, configure allow operations on a specific sensitive data (table or views). Block all other access and operations by creating a second **Database Object** rule. Ensure the blocking rule is the last one in the rule list.
Allow SQL statements from trusted IP addresses and applications	Deploy Database Firewall in **Monitoring / Blocking (Proxy)** mode. Configure the **Session Context** rule to allow SQL traffic from an allow list of client applications and their host IP addresses. Any other access must be monitored, alerted, or blocked by the Database Firewall using the **Default** rule. To enforce this database access pattern, create allow list in **Session Context** rule and configure the **Default** rule to alert or block other SQL statements.
Prevent SQL injection threats or zero day exploits	Deploy Database Firewall in **Monitoring / Blocking (Proxy)** mode. Configure the Database Firewall to capture SQL statements from trusted set of applications and database users. This is the allow list of SQL statements. Database Firewall uses a SQL grammar based engine to parse and group similar SQL statements into clusters. Create a list of such clusters and configure **SQL Statement** rule to all SQL statements matching the list for a specific target and alert or block SQL statements that have clusters not matching the list.
Detect potential data exfiltration attempts	Configure the Database Firewall policy to identify potential data exfiltration attempts by capturing the number of rows returned by the database in response to `SELECT` SQL queries using **Database Object** rule (starting from Oracle AVDF 20.3). For example, raise an alert if the number of returned rows exceeds a specific expected threshold on a specific sensitive table.

7.3 Types of Database Firewall Policies

Learn about the types of Database Firewall policies.

Database Firewall policies are categorized into:

- **User-defined Database Firewall Policies**
- **Pre-defined Database Firewall Policies**

User-defined Database Firewall Policies

Oracle AVDF allows you to define your own policies quickly and efficiently. There are 6 types of rules that you can create in these policies.

Rule	Description

Session Context	Client program session attributes like, client program name, host IP address, OS user, and database user are used to define the action of the Database Firewall in this rule.
SQL Statement	SQL statements captured by Database Firewall are clustered into groups of similar statements. This rule defines the action of the Database Firewall on such SQL clusters.
Database Object	Database Object rule defines the action of the Database Firewall based on SQL statement types (DML, DDL, etc.) on a list of configured tables or views.
Login/Logout	The login or logout rule defines the action of the Database Firewall based on login and logout sessions by client programs on target databases.
Unknown Traffic	This rule defines the action of the Database Firewall for SQL statements that are not recognized for the following possible reasons: • Database Firewall is unable to parse the SQL statement • Semantics of SQL statement is not valid • Communication protocol used by the client program and the target database is not supported by Database Firewall **Note:** Interpretation of Java code is not supported by Database Firewall.
Default	In this rule if a SQL statement does not meet any of the previous configured rules, then the Database Firewall acts as per the actions of this rule.

Pre-defined Database Firewall Policies

Oracle AVDF includes pre-defined Database Firewall policies. These define the frequency of logging SQL statements in Audit Vault Server. They only monitor the SQL statements and do not raise alerts or block SQL statements. For alerting or blocking SQL statements, **User-defined Database Firewall Policies** should be configured.

Policy Name	Description
Default	When Database Firewall monitoring point is configured for the target, this **Default** policy is applied automatically. This is available starting with Oracle AVDF release 20.7. The auditor can also assign this **Default** policy to existing Database Firewall monitoring points. The **Default** policy consists of the following three rules:

	1. **Login/Logout** rule that logs all login and logout events on the database with minimal threat severity. 2. **Monitor DDL and DCL Activity** rule that logs unique DDL and DCL statements. **Note:** Prior to Oracle AVDF 20.8, this rule was called **Log Sensitive Activity** 3. Pass all the remaining traffic without logging. Additionally the traffic is logged with data masking turned on to avoid accidental logging of sensitive data. This policy is applied by default to all new targets during registration. This includes all the new monitoring points configured later for the specific target database. This **Default** policy can be copied and customized like any other policy. **Note:** In case of upgrade from any release prior to Oracle AVDF 20.7, the Database Firewall monitoring points created prior to the upgrade will continue to have the same Database Firewall policy assigned prior to the upgrade. This **Default** policy can be applied after the upgrade.
Log all	Log all statements for offline analysis. All statements are logged in the Audit Vault Server. **Note:** If this policy is applied, it can use significant amount of storage for the logged data.
Log all - no mask	Log all statements for offline analysis without masking the data. Every statement is logged into Audit Vault Server without masking the data. **Note:** If this policy is applied, then it can use significant amount of storage for the logged data. Sensitive information may be logged if you select this policy.
Log sample	Log a sample of statements for offline analysis. The frequency of logging into Audit Vault Server is every tenth statement having the same cluster ID. **Note:** If this policy is applied, then it stores fewer statements than logging all statements. It can still use significant amount of storage for the logged data.
Log unique	Log examples of statements for offline analysis for unique SQL traffic. Unique statements are logged into Audit Vault Server. A SQL statement is considered as unique based on the following parameters:

	1. Cluster ID of the SQL statement 2. IP address of the client program 3. Database user 4. The uniqueness is calculated for a time interval of one hour for a specific session **Note:** If this policy is applied, then it stores fewer statements than logging all statements. It can still use significant amount of storage for the logged data.
Log unique - no mask	Log examples of statements for offline analysis covering unique SQL traffic without masking data. This is the same as "Log unique" excluding masking of data. **Note:** If this policy is applied, then it stores fewer statements than logging all statements. It can still use significant amount of storage for the logged data. Sensitive information may be logged if you select this policy.
Pass all	Pass all statements. No statements are logged into the Audit Vault Server.

7.4 Developing a Database Firewall Policy

Learn about developing a Database Firewall policy.

Developing a Database Firewall policy involves the following steps:

1. Creating a new Database Firewall policy.
2. Configuring the created Database Firewall policy.
3. Publishing a Database Firewall policy.
4. Deploying Database Firewall Policies to targets.
5. Exporting and Importing Database Firewall Policies

> **Note:**
>
> - All these operations are performed using the Audit Vault Server console.
> - In Oracle AVDF 20.3 and later, after the Database Firewall policy is created, it is published automatically.

7.5 Creating a New Database Firewall Policy

Learn about creating a Database Firewall policy.

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

3. Click **Database Firewall Policies** tab in the left navigation menu.

   Though this page lists your **User-defined Policies** and the **Oracle Pre-defined Policies**, only **User-defined Policies** can be created.

4. Click **Create** button.

   The **Create Policy** dialog appears.

5. Select the **Target Type** from the drop down list.
6. Enter a **Policy Name**. The name can't include `#` or `:`.
7. Optionally, enter **Description**. The description can't include `#` or `:`.
8.

In release	Action
20.1 - 20.2	Click **Save** and then click **Publish**.
20.3 - 20.7	Click **Save**.
20.8 - 20.9	Click **Save and Publish**.
20.10 and later	Click **Save**.

   After taking the appropriate action for your release, you will be brought to the policy details page. Here you will configure the policy.

7.6 Configuring the Created Database Firewall Policy

Learn about configuring the Database Firewall policy already created.

Configuring the Database Firewall policy involves:

1. Configuration of global policy settings.
2. Creation of sets or profiles.
3. Configuration of user defined rules.

7.6.1 Configuring Database Firewall Global Policy Settings

Learn how an auditor can configure or define an existing Database Firewall policy settings.

Global Policy settings in a Database Firewall represents the configuration settings applied to all the rules for a specific policy.

Prerequisite: Global Database Firewall settings can be configured after the policy is created.

1. Log in to the Audit Vault Server console as an *auditor*.
2. Select the **Policies** tab.
3. From the left navigation menu, click **Database Firewall Policies**.
4. In this page, click the name of the specific policy.
5. Click **Configuration** button in the top right corner. The following policy rules are displayed in different tabs:
   1. **Login / Logout**
   2. **Sensitive Data Masking**
   3. **Unknown Traffic**

   d. **Policy Pattern**

6. For example, click **Policy Pattern** tab. In this tab, configure the following:
   a. Under **Log Pattern** section, select whether to **Strip binary objects and comments from log files**.
   b. Under **Action Rule Pattern** section enter the **Threshold action reset time (minutes)** field. Enter a number in 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. In the **Action without substitution** 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 the **Syntax Rule Pattern** section, 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. For **Case sensitive match**, select whether this firewall policy does case sensitive matching for **Client program name**, **Database username**, and **Operating system username**.
7. Click **Save**.

7.6.1.1 Configuring Policies for Login and Logout Events

Learn how to configure Database Firewall policy for login and logout events.

You can specify login and logout policies for database users. For example, configure to raise alerts or block database users who make a specified number of unsuccessful login attempts.

Prerequisite: In order to use a login or logout policy for a target database, you must activate database response monitoring when configuring the Database Firewall monitoring point for the specific target database.

To configure the login and logout policies:

1. Log in to the Audit Vault Server console as an *auditor*.
2. Click **Policies** tab.
3. From the left navigation menu, click **Database Firewall Policies**.
4. Click the name of the specific policy.
5. In the **Policy** section, click **Configuration** button in the top right corner.
6. Under the **Login/Logout** tab and **Login** section, configure the following:
   a. **Action**: Specify the action for login sessions.
   b. **Threat Severity**: Select the severity level for successful or unsuccessful database user logins.
   c. **Set Logging**: Check this box to enable logging for logins and to view login session information in reports and alerts.
   d. **Failed Login**: Optionally, select the checkbox **Set failed login policy threshold**.

   This setting lets you produce an alert, or block a client program, after exceeding a specified number of consecutive unsuccessful logins. You can set a threshold and action.

If the threshold limit is reached, the login sessions are blocked for the specified **Reset Period (in seconds)**. After this period, the client program login attempts are passed to the target database.

> **Note:**
>
> Blocking a client program session after exceeding a specified number of consecutive unsuccessful logins is supported in **Monitoring / Blocking (Proxy)** deployment mode only.

7. Under the **Logout** section, configure the following:
   a. **Action**: Specify the action on logout sessions (whether to pass or alert).
   b. **Threat Severity**: Select the severity level for successful or unsuccessful database user logouts.
   c. **Set Logging**: To view logout session information in reports or alerts.
8. Click **Save** in the top right corner.

7.6.1.2 Configuring Policies for Masking Sensitive Data

Learn how to configure Database Firewall policy for masking sensitive data.

Database Firewall obfuscates passwords, string literals, and numerical constants by default for all SQL statements before logging in to the Audit Vault Server. In addition, the rules can be set for masking selective SQL statements. Data masking prevents sensitive and confidential data, such as credit card numbers from appearing in the log files, reports, and alerts. If a logged statement matches the data masking policy, the policy automatically replaces all user data in that statement.

Database Firewall masks the data depending on the data type:

- Delimited strings are masked as "`#`".
- Passwords are masked as `XXX`.
- String literals are masked as "`#`". String literals can be user names.
- All numerical constants like float, hexadecimal, decimal, integer, and binary constants are masked as "0" (zero). Numerical constants can be user ID.

> **Note:**
>
> After the data is masked by Database Firewall, it cannot be unmasked.

To set rules for data masking:

1. If you selected to mask based on criteria, enter the details as follows:

   Columns:

   - Choose from the list.
   - Or enter a database column name from the list of options available. Data masking is applied on the statements containing these columns.

- To remove one or more column names that are selected, click on the cross mark ("x") next to them. Accordingly the SQL statements are masked.

Procedures:

- Enter a procedure name and select from the list of options available to add the procedure name to the **Procedures** list. Data masking is applied on statements containing the specified procedures.
- To remove one or more procedure names that are selected, click on the cross mark ("x") next to them. Accordingly the SQL statements are masked.

1. Log in to the Audit Vault Server console as an *auditor*.
2. Click **Policies** tab.
3. From the left navigation menu, click **Database Firewall Policies**.
4. Click the name of a specific policy.
5. Click **Configuration** button in the top right corner.
6. Click **Sensitive Data Masking** tab.
7. Select or deselect the **Mask logged data** check box.
8. Select one of the following options:
   a. **For all statements**: This is the default selection.
   b. **For all statements matching the following criteria**: If you select to mask based on criteria, then enter the details as follows:

   Columns:

   - Use the search dialog, choose from the list, and click the **Add** button to add to the list. Data masking is applied on the SQL statements listed in these columns.
   - To remove one or more column names, select them and click the **Remove** button. Accordingly the SQL statements are masked.

   Procedures:

   - If it is left empty, data masking is applied on SQL statements containing any procedure.
   - Use the search dialog, choose from the list, and click the **Add** button to add to the list. Data masking is applied on the SQL statements listed in these columns.
   - To remove one or more procedure names, select them and click the **Remove** button. Accordingly the SQL statements are masked.
9. Click **Save**.

7.6.1.3 Configuring Policies for Unknown Traffic

Learn how to configure Database Firewall policy for unknown traffic.

Database Firewall policy rules can be configured for SQL statements that are not recognized for the following possible reasons:

- Database Firewall is unable to parse the SQL statement
- Semantics of SQL statement is not valid
- Communication protocol used by the client program and the target database is not supported by Database Firewall

> **Note:**
>
> Interpretation of Java code is not supported by Database Firewall.

To set the policy rules for unknown traffic:

1. Log in to the Audit Vault Server console as an *auditor*.
2. Select the **Policies** tab.
3. Select **Database Firewall Policies** in the left navigation menu.
4. Click the name of the specific policy. The details of the policy are displayed on the page.
5. Click **Configuration** button in the top right corner.
6. Click **Unknown Traffic** sub tab in the main page.
7. Assign the **Action**, **Logging Level**, and **Threat Severity** accordingly.
8. Optionally select **Set threshold for escalating action** checkbox to apply relevant action after unknown traffic statements exceed the number of times specified as the threshold limit. Then, enter the following
   a. **Threshold**: Enter the number of times unknown traffic must be seen before the escalation action is taken.
   b. **Threshold Time (in seconds)**: Set the threshold time.
   c. **Threshold Action**: Select `Alert` or `Block` as the action taken after the threshold is met.
   d. **Substitution SQL (Optional)**: When `Block` is selected for **Threshold Action**, enter a SQL statement to substitute for the unknown SQL statement.

   > **See Also:**
   >
   > Blocking SQL and Creating Substitute Statements

7.6.1.4 Configuring Database Firewall Policies for Policy Pattern

Learn how to configure Database Firewall policy rules for patterns in the SQL statements.

To set the policy rules for different patterns:

1. Log in to the Audit Vault Server console as an *auditor*.
2. Select the **Policies** tab.
3. Select **Database Firewall Policies** in the left navigation menu.
4. Click the name of the specific policy. The details of the policy are displayed on the page.
5. Click **Configuration** button in the top right corner.
6. Click **Policy Pattern** tab.
7. In this tab, configure the following:

Pattern Type	Action

Log Pattern	Select the option **Strip binary objects and comments from log files** checkbox to strip binary objects and comments from SQL statements before logging them into Audit Vault Server.
Action Rule Pattern	a. In the **Threshold action reset time (minutes)** field, enter an integer for the 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 is not repeated for the time specified here. This prevents too many block or warn actions for the same rule. b. In the **Action without substitution** field, select one of the actions (`No response` or `Drop connection`) if any of the Database Firewall policy rules is set to `Block`, and you have not specified a substitute statement in the rule.
Syntax Rule Pattern	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. For **Case sensitive match** select whether this policy does case sensitive matching for the following: a. **Client program name** b. **Database username** c. **Operating system username**

8. Click **Save**.

7.6.2 Creating And Managing Database Firewall Sets and Profiles

Learn how an auditor creates and manages Database Firewall sets and profiles.

When defining the Database Firewall policy rules, you should consider actors like Database Administrators, client programs, actions they can perform, or they cannot perform. Configure Database Firewall policy rules to take relevant actions based on actors and their actions. These actors are nothing but session context attributes retrieved by Database Firewall from the network traffic when a client program establishes a session with the target database.

These sets allow you to create a list of session context attributes such as client host IP addresses, database users, OS users, database objects, and client programs. You can also create sets of SQL clusters. SQL clusters are a group of SQL statements which are similar to each other. A profile is a named combination of sets.

Related Topics

- Managing Global Sets/Data Discovery
  Oracle AVDF 20.9 introduced Data Discovery which allowed the creation of global Privileged User and Sensitive Object sets on Oracle Database targets. In Oracle AVDF 20.10 this functionality was renamed to Global Sets and expanded to additionally allow the creation of global IP Address, OS User, Client Program, and Database User sets.
- Creating And Managing Database Firewall Sets and Profiles
  Learn how an auditor creates and manages Database Firewall sets and profiles.

- Creating a New Database Firewall Policy
  Learn about creating a Database Firewall policy.

7.6.2.1 Creating Sets

Learn about the types of sets and how to create them.

The following are the types of sets that can be configured and used in the rules:

1. **IP Address Sets**: A list of IP addresses of client programs (IPv4 format).
2. **Database User Sets**: A list of database user names.
3. **OS User Sets**: A list of operating system user names.
4. **Client Program Sets** (**Database Client Sets** in Oracle AVDF 20.3 and earlier): A list of client programs. For example SQL*Plus.
5. **Database Object Sets**: A list of tables to be evaluated by a policy.
6. **SQL Cluster Sets**: A list of SQL clusters. A SQL cluster is a group of SQL statements created automatically by Database Firewall that are similar, from the network traffic.

To create local sets:

1. Log in to the Audit Vault Server console as an *auditor*.
2. Select the **Policies** tab.
3. Select **Database Firewall Policies** in the left navigation menu.
4. Click the name of the specific policy. The details of the policy are displayed in the main screen.
5. Click **Sets/Profiles** in the top right corner. This page lists the sets already defined for the specific policy.
6. Click one of the following:
   - **IP Address Sets**
   - **Database User Sets**
   - **OS User Sets**
   - **Client Program Sets** (**Database Client Sets** in Oracle AVDF 20.3 and earlier)
   - **Database Object Sets**
   - **SQL Cluster Sets**
7. Click **Add** to add a new local set.
8. Use the dialog box to complete adding a new local set.

   > **Note:**
   >
   > If you're importing a file, it must be encoded in the UTF-8 format.

9. Click **Save**. The new local set appears in the specific policy page.
10. You can add more local sets by clicking on **Add** button for the specific set.

Starting with Oracle AVDF 20.9, see Managing Global Sets/Data Discovery to create global sets.

7.6.2.2 Creating and Managing SQL Cluster Sets

Learn how to create and manage SQL cluster sets in Database Firewall policy.

A SQL cluster set is a group of SQL clusters. SQL cluster is a group of SQL statements created automatically by Database Firewall which are similar to each other, from the network traffic.

You can create a new SQL cluster set as well as delete it. This deletes the definition only and does not remove the network data captured by the Database Firewall.

To create a SQL cluster set:

1. Log in to the Audit Vault Server console as *auditor*.
2. Select the **Policies** tab.
3. Select the **Database Firewall Policies** in the left navigation menu.
4. Click the name of the specific policy. The details of the policy are displayed in the main page.
5. Click **Sets/Profiles** in the top right corner. This page lists the existing sets that are already defined for the specific policy.
6. Click **SQL Custer Sets** sub tab.
7. To add a new SQL cluster set, click **Add**. The **Add SQL Cluster Set** dialog is displayed.
8. To get the list of SQL clusters, choose the filter options in the following fields:
   a. **Target**
   b. **Show cluster for**
9. Click **Go**. It displays all the SQL clusters depending on the selection.
10. Select the specific SQL clusters. To know the SQL statements associated with the cluster refer to the sample SQL from cluster column values.
11. Enter the **Name** and optionally **Description**.
12. Click **Save**. A new SQL cluster set is added and is listed in the **Sets/Profiles** page. More such sets can be added by following the above steps.

To add or delete the SQL cluster from a given set:

1. Click **SQL Cluster Sets** sub tab.
2. From the report choose the specific SQL cluster set, the details of the cluster set are displayed.
3. Choose **Add** and follow the procedure to add new clusters to an existing set.
4. From the same dialog, choose **Delete** option to delete one or more clusters from the set.
5. Click **Save**.

7.6.2.3 Creating and Managing Profiles

Learn how to create and manage profiles in Database Firewall policy.

A profile is a named combination of one or more of the below sets:

1. **IP Address Set**

2. **DB User Set**
3. **OS User Set**
4. **Client Program Set** (**DB Client Set** in Oracle AVDF 20.3 and earlier)

You can create a user with the profile. For example, you can create a system DBA profile using the **DB User Set**. This set can contain all the DBA users.

To create a profile:

1. Log in to the Audit Vault Server console as an *auditor*.
2. Select the **Policies** tab.
3. Select **Database Firewall Policies** tab in the left navigation menu.
4. Click the name of the specific policy.
5. Click **Sets/Profiles** button in the top right corner.
6. Click **Profiles** sub tab. This page lists the existing profiles. You can click a profile name to edit it.

> **Note:**
>
> Create a set first. It is not possible to create a profile without a set already existing.

7. Click **Add** to create a new profile.
8. In the **Add profile** dialog, enter the following:
   - **Name**: Enter a name for the profile.
   - **Description**: Optionally enter the description.
   - **IP Address Set**: From the list, select one of the available IP address sets, or leave it unselected.
   - **DB User Set**: From the list, select one of the available database user sets, or leave it unselected.
   - **OS User Set**: From the list, select one of the available operating system user sets, or leave it unselected.
   - **Client Program Set** (**DB Client Set** in Oracle AVDF 20.3 and earlier): From the list, select one of the available client program sets, or leave it unselected.

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

9. Click **Save**.

   The profile appears in the **Profiles** sub tab. You can now select this profile and set policy rules for the SQL Statements. Starting Oracle AVDF 20.4 and later the profile can be selected in a **Database Object** rule also.

7.6.3 Database Firewall Policy Rules

Learn about Database Firewall policy rules.

7.6.3.1 About Database Firewall Policy Rules

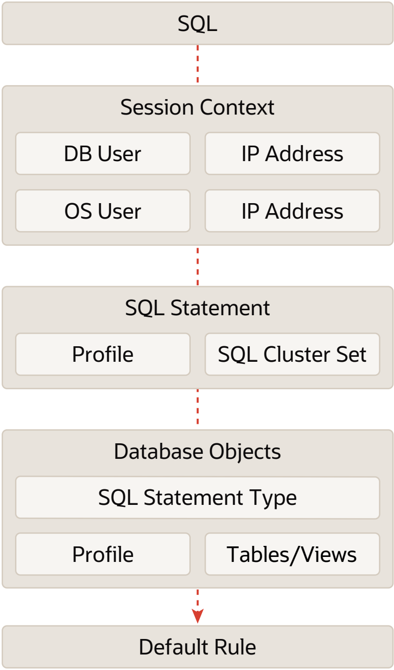
Learn about types of Database Firewall policy rules.

The following are the Database Firewall rule types:

- **Session Context**
- **SQL Statement**
- **Database Objects**
- **Default**

Policy Evaluation by Database Firewall

Figure 7-1 Order of Evaluation of Rules



Database Firewall is a multi stage engine that analyses and inspects SQL traffic to the database, extracts SQL statement from the traffic, and with a high precision determines whether to allow, alert, or block the SQL statement as specified in the policy. The SQL statement goes through different stages of analysis in the Database Firewall. This includes checks for originating IP address, database user name, OS user name, client program name, SQL statement category (DDL, DML, etc.), database tables, or views being accessed. This information can be used to determine whether the SQL statement can be allowed, requires raising an alert, or requires blocking.

Every stage has actions specified and checks carried out. In case there is a match, then the evaluation of the rule stops. **Session Context** rules are evaluated first. This is followed by **SQL Statements** and **Database Object** rules. In the last is the **Default** rule.

> **Note:**
>
> Profiles for **Database Object** rule in Database Firewall policy is introduced starting Oracle AVDF 20.4.

7.6.3.2 Evaluation Order of the Rules

Learn about the order in which the Database Firewall rules are evaluated or applied.

There can be multiple rules within a rule type. The table below lists the order in which they are applied or evaluated.

Rule Type	Oracle AVDF Release 20.3 and Earlier	Oracle AVDF Release 20.4 and Later
Session Context	Session Context rules are applied in the order they are listed in the policy overview page.	Session Context rules are applied in the order they are listed in the policy overview page.
SQL Statement	SQL Statement rules are applied in the order they are listed in the policy overview page.	SQL Statement rules are applied in the order they are listed in the policy overview page.
Database Object	Database Object can be configured with **ANY** or **ALL** tables. The matching is applied using either **ALL** or **ANY** operator as follows: 1. If **ALL** operator is selected, then the SQL statements must contain all the tables in the list. 2. If **ANY** operator is selected, then the SQL statements must contain at least one table from the list. **ANY** rules are evaluated first, and then **ALL** rules.	Database Object rules are applied in the order they are listed in the policy overview page.
Default	Can contain one rule only.	Can contain one rule only.

In **Monitoring / Blocking (Proxy)** mode, by default the Database Firewall blocks all IPv6 traffic regardless of the policies in place.

Starting with Oracle AVDF 20.4, the evaluation order of the rules can be changed. Follow these steps:

1. Click **Evaluation Order** button. A dialog appears.
2. Change the order of the rules using the up or down arrows on the right.
3. Click **Save**. A confirmation message is displayed on the screen. The updated order of the rules is refreshed on the main page.

7.6.3.3 Session Context Rule

Learn about the **Session Context** rule.

A session from a SQL client program trying to connect to the target database, contains information like Host IP address, Database user name, operating system user name and client program name. These are referred as session context attributes. **Session Context** rule is applied on the session context attributes. For example, allowing SQL statements from a trusted allow list client IP address range. It also allows to block SQL statements originating outside the expected IP address range.

The following sets are used when creating the **Session Context** rule:

1. **IP Address Set**
2. **DB User Set**
3. **OS User Set**
4. **Client Program Set** (**DB Client Program** in Oracle AVDF 20.3 and earlier)

To create a session context rule:

1. Log in to the Audit Vault Server console as an *auditor*.
2. Select the **Policies** tab.
3. Select **Database Firewall Policies** in the left navigation menu.
4. Select the name of an existing custom policy, or click **Create** to create a new one.

   > **Note:**
   >
   > Though the page displays both **User-defined Database Firewall Policies** and **Oracle Pre-defined Database Firewall Policies**, only **User-defined Database Firewall Policies** can be created.

5. In the **Database Firewall Policy Rules** section, expand the **Session Context** section.
6. Click **Add**. The **Session Context** dialog is displayed.
7. Enter a **Rule Name** and optionally **Description**.
8. For the following fields listed under **Ruleset** section:
   a. **IP Address Set**: Select to include or exclude, and then select an IP address set from the list.
   b. **DB User Set**: Select to include or exclude, and then select a database user set.
   c. **OS User Set**: Select to include or exclude, and then select an OS user set.
   d. **Client Program Sets** (**DB Client Program** in Oracle AVDF 20.3 and earlier): Select to include or exclude, and then select a SQL client program.

   > **Note:**
   >
   > - There is no limit on the number of items that can be included in these sets.
   > - You can use `*` (asterisk) as a wildcard for all the sets except **IP Address Set**.
   > - There is an option in all the sets to make it case sensitive or otherwise. This can be done by selecting or deselecting the check box in the global policy configuration, and selecting **Policy Pattern**, and then **Case sensitive match**.
   > - For example, if you select to include an **IP Address Set**, and exclude a **DB User Set**, then this **Session Context** rule will only apply to SQL traffic from the selected **IP Address Set**. However, it does not apply to the SQL traffic from the database users in the selected **DB User Set**.

9. Select the appropriate options available in the following fields under **Action** section:

   a. **Action**
   b. **Logging Level**
   c. **Threat Severity**
   d. Optionally select **Set threshold for escalating action** if you want to apply a different escalation action after a threshold. Enter the following:
      i. **Threshold**: Enter the number of times SQL match must exceed before the escalation action is taken.
      ii. **Threshold Time (in seconds)**
      iii. **Threshold Action**: Select `Alert` or `Block` as the action taken after the threshold is met.
      iv. **Substitution SQL**: (Optional) If you selected `Block` for the **Threshold Action**, enter a statement to substitute for the SQL statement matching this rule.
10. Click **Save**.

7.6.3.4 SQL Statement Rule

Learn about the **SQL Statement** rule.

Database Firewall extracts and analyzes SQL statements from network traffic. It groups similar SQL statements into clusters. Such clusters can be further grouped to form cluster sets. **SQL Statement** rule is used to configure actions that the Database Firewall must take on a SQL statement belonging to cluster sets.

Allow list (white list) or deny list based policies can be created using this rule. The allow list of SQL clusters can be created by sending known or expected SQL statements from trusted applications over a period of time. Include allow list of SQL cluster sets and configure to allow SQL statements with clusters belonging to the allow list, when creating the **SQL Statement** rule.

Make use of profiles to create a deny list based policy. For example, create cluster sets for sensitive data, and then create a profile of database administrators (DBA). Configure a rule to block SQL statements from DBA profile users with clusters matching the created cluster set. In this case the rule works as deny list.

To create a **SQL Statement** rule:

1. Log in to the Audit Vault Server console as an *auditor*.
2. Select the **Policies** tab.
3. Click **Database Firewall Policies** in the left navigation menu.
4. Click the name of an existing policy or click **Create** to create a new one.
5. Expand the **SQL Statement** section.
6. Click **Add**.
7. In the **SQL Statement** dialog, enter a **Rule Name**.
8. Optionally enter the **Description**.
9. Select the **Profile** from the list.
10. In the **Cluster Set(s)** field, select the cluster in the **Available** column and move to the **Selected** column. Refer to the section on how to create cluster sets. Create a cluster set prior to creating a policy rule for **SQL Statement**.

11. In the **Action** section, enter the details for **Action**, **Logging Level**, and **Threat Severity** fields to apply to SQL statements of this cluster type.
12. Optionally select the checkbox for **Set threshold for escalating action** field, if an action is required on the SQL statement that matches this cluster threshold times. Upon selecting this checkbox, 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 Time (in seconds)**: Enter the time in seconds.
    c. **Threshold Action**: Select `Alert` or `Block` as the action taken after the threshold is met.
    d. **Substitution SQL**: If you selected `Block` for the **Threshold Action**, then enter a statement to substitute for the SQL matching this rule.
13. Click **Save**.

7.6.3.5 Database Object Rule

Learn about the Database Object rule.

Database Object rules are used to allow, alert or block specific types of SQL statements (DML, DDL, etc.) on specific database objects such as tables and views. These rules are often used for controlling access to sensitive application data.

Database Object rule can be used in the following scenarios:

- Monitoring specific statement types that are of interest on sensitive tables. Use **Any** table field, and select `TRANSACTION COMPOSITE` under **Statement Classes**. You can also select the tables `AVG_COST`, `BOOKS`, and `BUSINESS_CONTACTS`. A statement that matches this rule must be `TRANSACTION COMPOSITE` and it can contain any of the tables selected.
- Monitoring specific statement types that are of interest on sensitive tables, by using **All** table field. Select `Procedural` and `Composite` under **Statement Classes**. You can also select the tables `AVG_COST`, `BOOKS`, and `BUSINESS_CONTACTS`. A statement that matches this rule must either be `Procedural` or `Composite`, and the SQL statement must have all the tables (`AVG_COST`, `BOOKS`, and `BUSINESS_CONTACTS`).
- Monitoring exfiltration attempts of sensitive data. Use this functionality by creating a **Database Object** rule to capture the number of rows returned by a `SELECT` query. Select `Data Manipulation Read only` under the **Statement Classes** field. This option is available only for `Data Manipulation Read only` statement class. **All** or **ANY** tables can be selected according to the requirement. This data is further available for selection in the **All Activity** and **Database Firewall Reports**. Alerts can be configured if the returned number of rows exceeds a threshold value.

- Oracle AVDF Release 20.1-20.8
- Oracle AVDF Release 20.9 and 20.10
- Oracle AVDF Release 20.11 and later

Oracle AVDF Release 20.1-20.8

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

2. Select the **Policies** tab.
3. Click **Database Firewall Policies** tab in the left navigation menu.
4. Click the name of an existing user-defined policy . The page specific to that policy appears.

> **Note:**
>
> Though the page displays both **User-defined Database Firewall Policies** and **Oracle Pre-defined Database Firewall Policies**, only **User-defined Database Firewall Policies** can be altered.

5. Expand the **Database Objects** section, and then click on an existing database object rule or click **Add**. The **Database Objects** dialog is displayed.
6. Provide a **Rule Name**.
7. Enter a **Description**.
8. Select a **Profile**, the default is none as shown by **-**.
9. In the **Statement Classes**, select one or more types of statement classes that SQL statements must match in order to apply this rule.
10. If the target type is an Oracle Database and one of the values for the **Statement Classes** field is `Data Manipulation Readonly` (Prior to Oracle AVDF Release 20.4) or `SELECT` (Oracle AVDF Release 20.4 and later), the field **Capture number of rows returned for SELECT queries** is able to be toggled to `Yes`. Upon setting this field to `Yes`, it captures the number of rows for select queries as per the policy, and displays in the **All Activity** and **Database Firewall Reports** under the column **Row Count**. This column will be available for selection in the reports. Alerts can be configured for the number of rows fetched or queried.
11. Select the tables to be monitored in the **Tables/Views to be monitored** section. You will see a preview of the selected tables if you've already chosen which tables to monitor.

> **Note:**
>
> All Tables and Views are monitored unless specified.

    a. To edit the list of tables to be monitored, click the pencil icon to the right of the text box.
    b. In the dialog box you can edit the list of tables to be monitored from the three tabs: **Enter Values**, **From File**, or **From Collected Data**.

    - In the **Enter Values** tab, type the table names in the text box. You will need to enter each table or view on a separate line. Click **Save** once done.
        a. If left empty, all the tables analyzed by the Database Firewall are considered.
        b. Include fully qualified table names. **Note:** The tables `T1` and `Myschema.T1` are considered as different. Hence, include all tables names as appropriate.
    - In the **From File** tab, click the **Choose File** field to upload a `.txt` file containing the names of tables or views, with one name per line. Select your `.txt` file from the pop-up of your computer's files. Click **Save** once done.
    - In the **From Collected Data** tab, select tables from the **Available** column and move them to the **Selected** column using the filters in the middle. You can search for tables

by typing in the search box in the top left of the dialog. This will narrow down the list of visible tables under the **Available** column. Click **Save** once done.

- (Optional) At the bottom of each tab is a table called **Tables/Views to be monitored**. This table contains the selected tables or views that will be monitored. An empty list means all tables and views are monitored. To select all tables and views, select the check box to the left of the **Tables/views** column header. To select any tables and views, select the check box to the left of the **Tables/views** column for that table or view. Click **Delete** to remove any selected table(s) or view(s) from the list to be monitored.

12. In the **Action to be taken** section, select the **Action**, **Logging Level**, and **Threat Severity** for this rule from the appropriate drop down list.
13. If you select `Block` as the **Action**, then the **Substitution SQL** field appears. Enter a statement to substitute for the SQL statement that was blocked.
14. Click **Save**.

Oracle AVDF Release 20.9 and 20.10

1. Log in to the Audit Vault Server console as an *auditor*.
2. Select the **Policies** tab.
3. Click **Database Firewall Policies** tab in the left navigation menu.
4. Click the name of an existing user-defined policy . The page specific to that policy appears.

> **Note:**
>
> Though the page displays both **User-defined Database Firewall Policies** and **Oracle Pre-defined Database Firewall Policies**, only **User-defined Database Firewall Policies** can be altered.

5. Expand the **Database Objects** section, and then click on an existing database object rule or click **Add**. The **Database Objects** dialog is displayed.
6. Provide a **Rule Name**.
7. Enter a **Description**.
8. Select a **Profile**, the default is none as shown by **-**.
9. In the **Statement Classes**, select one or more types of statement classes that SQL statements must match in order to apply this rule.
10. If the target type is an Oracle Database and one of the values for the **Statement Classes** field is `SELECT`, the field **Capture number of rows returned for SELECT queries** is able to be toggled to `Yes`. Upon setting this field to `Yes`, it captures the number of rows for select queries as per the policy, and displays in the **All Activity** and **Database Firewall Reports** under the column **Row Count**. This column will be available for selection in the reports. Alerts can be configured for the number of rows fetched or queried.
11. In the **Tables/Views to be monitored** section, select one of the global or local sets from the **DB Object Set** drop down.
    Database object sets can be global or local sets. Global sets can be viewed in and applied to multiple database firewall policies, whereas local sets can only be viewed in and applied to the database firewall policies they were created in. Global sets can be created in Managing Global Sets/Data Discovery.

> **Note:**
>
> All Tables and Views are monitored unless specified.

a. To add **Database Object Sets**, click the + button to the right of the text box.

b. In the dialog box you can edit the list of tables to be monitored from the three tabs: **Enter Values**, **From File**, or **From Collected Data**.

   - In the **Enter Values** tab, type the table names in the text box. You will need to enter each table or view on a separate line. Click **Save** once done.
     - If left empty, all the tables analyzed by the Database Firewall are considered.
     - Policy evaluation happens on the table irrespective of schema. For example, the policy will evaluate qualified table name, `Myschema.T1` and the plain table name, `T1` in the same manner.
     - Table names can also include wild card characters by using * in the table name. For example, `T*` will include `T1` and `T2`.
   - In the **From File** tab, click the **Choose File** field to upload a `.txt` file containing the names of tables or views, with one name per line. Select your `.txt` file from the pop-up of your computer's files. Click **Save** once done.
   - In the **From Collected Data** tab, select tables from the **Available** column and move them to the **Selected** column using the filters in the middle. You can search for tables by typing in the search box in the top left of the dialog. This will narrow down the list of visible tables under the **Available** column. Click **Save** once done.
   - (Optional) At the bottom of each tab is a table called **Tables/Views to be monitored**. This table contains the selected tables or views that will be monitored. An empty list means all tables and views are monitored. To select all tables and views, select the check box to the left of the **Tables/views** column header. To select any tables and views, select the check box to the left of the **Tables/views** column for that table or view. Click **Delete** to remove any selected table(s) or view(s) from the list to be monitored.

12. In the **Action to be taken** section, select the **Action**, **Logging Level**, and **Threat Severity** for this rule from the appropriate drop down list.
13. If you select `Block` as the **Action**, then the **Substitution SQL** field appears. Enter a statement to substitute for the SQL statement that was blocked.
14. Click **Save**.

Oracle AVDF Release 20.11 and later

1. Log in to the Audit Vault Server console as an *auditor*.
2. Select the **Policies** tab.
3. Click **Database Firewall Policies** tab in the left navigation menu.
4. Click the name of an existing user-defined policy . The page specific to that policy appears.

> **Note:**
>
> Though the page displays both **User-defined Database Firewall Policies** and **Oracle Pre-defined Database Firewall Policies**, only **User-defined Database Firewall Policies** can be altered.

5. Expand the **Database Objects** section, and then click on an existing database object rule or click **Add**. The **Database Objects** dialog is displayed.
6. Provide a **Rule Name**.
7. Enter a **Description**.
8. Select a **Profile**, the default is none as shown by **-**.
9. In the **Commands** section, select the specific commands to add to this rule
10. If the target type is an Oracle Database and one of the values for the **Commands** field is `SELECT`, the field **Capture number of rows returned for SELECT queries** is able to be toggled to `Yes`. Upon setting this field to `Yes`, it captures the number of rows for select queries as per the policy, and displays in the **All Activity** and **Database Firewall Reports** under the column **Row Count**. This column will be available for selection in the reports. Alerts can be configured for the number of rows fetched or queried.
11. In the **Tables/Views to be monitored** section, select one of the global or local sets from the **DB Object Set** drop down.
    Database object sets can be global or local sets. Global sets can be viewed in and applied to multiple database firewall policies, whereas local sets can only be viewed in and applied to the database firewall policies they were created in. Global sets can be created in Managing Global Sets/Data Discovery.

    > **Note:**
    >
    > All Tables and Views are monitored unless specified.

    a. To add **Database Object Sets**, click the + button to the right of the text box.
    b. In the dialog box you can edit the list of tables to be monitored from the three tabs: **Enter Values**, **From File**, or **From Collected Data**.
        - In the **Enter Values** tab, type the table names in the text box. You will need to enter each table or view on a separate line. Click **Save** once done.
            – If left empty, all the tables analyzed by the Database Firewall are considered.
            – Policy evaluation happens on the table irrespective of schema. For example, the policy will evaluate qualified table name, `Myschema.T1` and the plain table name, `T1` in the same manner.
            – Table names can also include wild card characters by using * in the table name. For example, `T*` will include `T1` and `T2`.
        - In the **From File** tab, click the **Choose File** field to upload a `.txt` file containing the names of tables or views, with one name per line. Select your `.txt` file from the pop-up of your computer's files. Click **Save** once done.
        - In the **From Collected Data** tab, select tables from the **Available** column and move them to the **Selected** column using the filters in the middle. You can search

for tables by typing in the search box in the top left of the dialog. This will narrow down the list of visible tables under the **Available** column. Click **Save** once done.

- (Optional) At the bottom of each tab is a table called **Tables/Views to be monitored**. This table contains the selected tables or views that will be monitored. An empty list means all tables and views are monitored. To select all tables and views, select the check box to the left of the **Tables/views** column header. To select any tables and views, select the check box to the left of the **Tables/views** column for that table or view. Click **Delete** to remove any selected table(s) or view(s) from the list to be monitored.

12. In the **Action to be taken** section, select the **Action**, **Logging Level**, and **Threat Severity** for this rule from the appropriate drop down list.
13. If you select `Block` as the **Action**, then the **Substitution SQL** field appears. Enter a statement to substitute for the SQL statement that was blocked.
14. Click **Save**.

Here are some important points to note for capturing return number of rows for `SELECT` queries feature:

- This functionality is applicable for **Database Objects** rule in release Oracle AVDF 20.3.
- This is applicable when Database Firewall is deployed in **Monitoring / Blocking (Proxy)** mode.
- This feature is available only for Oracle Database (version 12c and later).
- In Oracle AVDF 20.3 it is recommended not to enable **Capture Database Response** field if you are planning to use this functionality. This limitation has been removed in Oracle AVDF 20.4 and later.
- This functionality does not support use of cursors and partial data fetch.
- This functionality is supported on all 64 bit operating systems.
- This functionality can be used with JDBC driver based clients, SQL*Plus, and other Oracle DB OCI based clients.
- In case the return row count information does not show in reports, then review the traffic log timer. See *Retrieval of Row Count Does Not Work* for more information.
- While configuring a **Database Object** rule, consider the tables for which the return row count feature needs to be enabled. It is recommended to enable the return row count option on `SELECT` queries that operate on a single table. Composite queries on multiple tables can raise false positives. Use **ANY** or **ALL** selection as per the requirement.
- A malicious user may use different ways to hide data exfiltration. One of them may be partial fetches of the result set. Database Firewall marks the row count with value `-1` for such cases. It is recommended to configure alerts based on this behavior.

Related Topics

- Statement Class to Command Mappings for Database Firewall Policies

7.6.3.5.1 Statement Class to Command Mappings for Database Firewall Policies

Starting in Oracle AVDF 20.11, Database Firewall policies no longer utilize statement classes. Instead, users are able to create policies based on specific commands such as `INSERT`, UPDATE, or DELETE. This table can help you identify which commands are a part of which statement class.

Statement Class	Commands for Oracle	Commands for SQL Server	Commands for MySQL	Commands for DB2 LUW	Commands for Sybase ASE
DCL	ADMINISTER, ALTER (DCL), ALTER SESSION, ALTER SYSTEM, COMPRESSED, ENCRYPTED, CHANGE PASSWORD, GRANT, INVALID OPERATION, LOGIN, ORADEBUG, REVOKE, SET ROLE, SHUTDOWN	ALTER AUTHORIZATION, DBCC, DENY, GRANT, LOGIN, REVOKE, SET, SETUSER, USE	BINLOG, FLUSH, GRANT, INSTALL, KEYCACHE, KILL, PURGE, RESET, REVOKE, SET ROLE, UNINSTALL, USE	GRANT, REVOKE, SET, TRANSFER	DBCC, GRANT, KILL, LOAD, LOCK, MOUNT, REVOKE, SET, SETUSER, SYSTEM, TRANSFER, USE
DDL	ALTER (DDL), ALTER AUDIT POLICY, ALTER DATABASE, ALTER PROFILE, ALTER TABLE, ALTER TABLESPACE, ALTER USER, ANALYZE, ASSOCIATE, AUDIT, COMMENT, CREATE, DISASSOCIATE, DROP, NOAUDIT, RENAME, TRUNCATE	ADD, ALTER(DDL), ALTER DATABASE, ALTER TABLE, ALTER USER, CREATE, DISABLE, DROP, ENABLE, RECONFIGURE, TRUNCATE	ALTER, CHECK, CHECKSUM, CREATE, DROP, PARTITION, RENAME, REPLACE, TRUNCATE	ALLOCATE, ALTER, COMMENT, CREATE, DROP, RENAME, TRUNCATE	ALTER, CREATE, DEALLOCATE, DROP, TRUNCATE

Statement Class	Commands for Oracle	Commands for SQL Server	Commands for MySQL	Commands for DB2 LUW	Commands for Sybase ASE
DML	`DELETE, EXECUTE CURSOR, EXPLAIN, FLASHBACK, INSERT, LOB WRITE, MERGE, PURGE, UPDATE`	`BACKUP, DELETE, INSERT, MERGE, RESTORE, UPDATE, UPDATETEXT, WRITETEXT`	`ANALYZE, DELETE, GET, INSERT, LOAD, OPTIMIZE, REPAIR, UPDATE`	`DELETE, EXPLAIN, INSERT, MERGE, REFRESH, UPDATE`	`DELETE, DUMP, EXECUTE CURSOR, INPUT, INSERT, MERGE, QUIESCE, REFRESH, REMOVE, REORG, UNMOUNT, UPDATE, WRITETEXT`
Procedural	`PROCEDURAL`	`PROCEDURAL`	`PROCEDURAL`	`PROCEDURAL`	`PROCEDURAL`
Select	`SELECT`	`SELECT`	`SELECT`	`SELECT`	`SELECT`
Transaction	`TRANSACTION`	`TRANSACTION`	`TRANSACTION`	`TRANSACTION`	`TRANSACTION`

> **Note:**
>
> Composite and Composite with Transaction statement classes do not have any equivalent commands, so they will not be displayed. If you had policies with these statement classes prior to upgrading to Oracle AVDF 20.11 or later, no commands will get automatically added to the policy during upgrade.

7.6.3.6 Default Rule

Learn about the **Default** rule.

The **Default** rule specifies the action for any SQL statement that does not meet the criteria of any previous policy rules. When the Database Firewall observes such a statement, the **Default** rule is applied. The default configuration is to allow the SQL statements without logging them into the Audit Vault Server. A different action in the **Default** rule can applied along with a substitute statement (optional in case **Block** action is considered).

To configure the **Default** rule:

1. Optionally select **Set threshold for escalating action** field, if you want to apply a different action after statements fall within the default rule a number of times. Then enter the following:
2. Click **Save**.

> **See Also:**
>
> Blocking SQL and Creating Substitute Statements

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

2. Click on **Policies** tab.
3. Click **Database Firewall Policies** in the left navigation menu.
4. Click the name of an existing policy or click **Create** to create a new one.
5. Expand the **Default**section on the main page.
6. Click **Default Rule**.
7. In the **Default** dialog, select the values for **Action**, **Logging Level**, and **Threat Severity** fields.
8. Optionally select **Set threshold for escalating action** field. Then, enter the following:
    a. **Threshold**: Enter the number of times a SQL statement must fall within the **Default** rule before the escalation action is taken.
    b. **Threshold Time (in seconds)**: Enter the time in seconds.
    c. **Threshold Action**: Select `Alert` or `Block` as the action taken after the threshold is met.
    d. **Substitution SQL**: (Optional) If `Block` is selected for the **Threshold Action** field, then enter a substitute for the SQL statement matching this rule.
9. Click **Save**.

7.7 Publishing and Deploying Firewall Policies

Learn how to publish and deploy firewall policies.

7.7.1 About Publishing and Using Database Firewall Policies

You can edit a Database Firewall policy until it is published.

Publishing a policy makes it available to deploy on targets.

After a Database Firewall policy is deployed on a target, it cannot be edited. However, you can copy the policy and edit the same with another name. After completely editing the Database Firewall policy, it can be published and assigned to the targets.

7.7.2 Publishing a Database Firewall Policy

Learn how to publish a Database Firewall policy as an auditor.

Follow these steps to publish a Database Firewall policy in Oracle AVDF release 20.2 and earlier:

1. Log in to the Audit Vault Server console as an *auditor*.
2. Select the **Policies** tab.
3. From the left navigation menu, click **Database Firewall Policies**.
4. Click the check box against the specific policy.
5. Click **Save and Publish**.

    A Database Firewall policy publish job is started. A confirmation message is displayed on the screen.
6. Check the status of the published job by navigating to the **Settings** tab, and then clicking the **Jobs** tab in the left navigation menu.

7. After the policy is published, it is available in the **Database Firewall Policies** tab in the left navigation menu.

> **Note:**
>
> In Oracle AVDF 20.3 and later, after the Database Firewall policy is saved, it is published. The **Publish** button does not exist in Oracle AVDF release 20.3 and later. Navigate to the policy details page and click **Save and Publish** to publish.

7.7.3 Deploying Database Firewall Policies

Learn how to deploy database firewall policies through either the **Policies** or **Targets** tab.

Starting with release 20.8, database firewall policies can be deployed from the **Policies** tab. Database firewall policies can also be deployed from the **Targets** tab.

7.7.3.1 Deploying Database Firewall Policies from Policies Tab

Learn how to deploy either User-defined or Pre-defined Database Firewall Policies directly from the **Policies** tab in Oracle Audit Vault and Database Firewall.

Starting with Oracle AVDF release 20.8, Database Firewall policies can be deployed to target databases directly from the **Policies** tab. The process is the same for **User-defined Policies**and **Oracle Pre-defined Policies**.

1. In the table of policies, select the policy you wish to deploy by clicking the check box to the left of the **Policy Name** column.

   Note: You can only deploy one policy at a time so only select one policy.

2. Click the **Deploy** button in the top right of either the **User-defined Database Firewall Policies** or **Pre-defined Database Firewall Policies** section depending on what type of policy you are deploying.

   In the pop-up box that appears you will see:

   - The name of the policy you selected next to **Policy Name**
   - The database type of the policy you selected next to **Type**
   - A table of target databases that are of the selected **Type**

3. Optional: If the policy you selected has multiple target database types, you can filter the list of target databases by clicking on the drop down arrow next to **Type** and selecting a database type.

4. Optional: You can search for target databases that are of the selected **Type** by entering the database name into the text field above the table of target database and clicking **Go**.

5. Select which target database(s) you would like to deploy the selected policy to by clicking the check boxes to the left of the **Target Name** column.

   Note: Though you may select multiple target databases to deploy a policy to, they must be of the same database type.

6. Click **Deploy** in the bottom right of the pop-up box to finish deploying the selected Database Firewall Policy to your target database(s).

7. Click **Cancel** in the bottom right or the **X** in the top right of the pop-up box to cancel deploying the selected Database Firewall Policy.

7.7.3.2 Deploying Database Firewall Policies from Targets Tab

Learn how to deploy a Database Firewall policy to target databases from the Targets tab.

To deploy a Database Firewall policy:

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

   Prior to Oracle AVDF 20.7, log in as a `super auditor`.
2. Click **Targets** tab.
3. Click **Database Firewall Monitoring** tab in the left navigation menu.
4. Click on the name of the specific target.
5. In the target details page, click **Database Firewall Monitoring** tab.
6. Scroll down in this section and click the edit icon under the **Database Firewall Policy** section.
7. From the drop down list, select the policy.
8. Click the check mark.

7.8 Exporting and Importing Database Firewall Policies

Learn how to export and import one or more Database Firewall policies.

Starting in Oracle AVDF release 20.7, **User-defined Database Firewall Policies** in one Audit Vault Server instance can be exported and later imported to another Audit Vault Server instance. This saves time in creating the same policies across multiple Audit Vault Server instances.

For example, the **User-defined Database Firewall Policies** can be exported and imported between:

1. Test to production Audit Vault Server instance.
2. Primary Audit Vault Server instance to DR (Disaster Recovery) Audit Vault Server instance.

When exported the Database Firewall policy can be downloaded and stored into a file in JSON format in Oracle AVDF release 20.7 or in a proprietary encrypted binary format starting in Oracle AVDF release 20.8. This file contains all the data and can be used to import later. This file is protected with a password defined by the user. The same password has to be entered to view the policy details and also during the import process.

> **Note:**
>
> This functionality is not applicable to **Pre-defined Database Firewall Policies** as they are available on all the Audit Vault Server instances and can easily be selected.

Prerequisites

- To export or import Database Firewall policies, the user must have auditor privileges assigned.
- A **User-defined Database Firewall Policy** must be first published in order to be exported.

7.8.1 Exporting Database Firewall Policies

Learn how to export one or more Database Firewall policies.

1. Log in to the Audit Vault Server console as an *auditor*.
2. Click **Policies** tab.
3. Click **Database Firewall Policies** tab in the left navigation menu.
4. Select one or more custom policies using the check box against the policies. These policies must be published in order to be exported.

> **Note:**
>
> Though the page displays both **User-defined Database Firewall Policies** and **Oracle Pre-defined Database Firewall Policies**, only **User-defined Database Firewall Policies** can be exported.

5. Click the **Export** button in the top right corner of the page.
6. In the **Export Policy** dialog, enter the password. The password requirement is similar to other passwords in the Audit Vault Server.
7. Click **Save**.
8. Specify a location to save the file when prompted.
9. In Oracle AVDF release 20.7 the file is saved as a JSON in the specified location as a bundle (`.zip` file) and is protected with a password. Starting with Oracle AVDF release 20.8, the Database Firewall policy file is in a proprietary encrypted binary format and is saved in the specified location and is password protected.

> **See Also:**
>
> Password Requirements

7.8.2 Importing Database Firewall Policies

Learn how to import one or more Database Firewall policies.

1. Log in to the Audit Vault Server console as an *auditor*.
2. Click **Policies** tab.
3. Click **Database Firewall Policies** tab in the left navigation menu.
4. Click the **Import** button in the top right corner of the page.
5. In the **Import Policy** dialog, click and navigate to choose the JSON file that contains all the details of the Database Firewall policies. In Oracle AVDF release 20.7, the JSON file that contains the Database Firewall policy details is a password protected bundle (`.zip` file). Starting with Oracle AVDF release 20.8, the Database Firewall policy is exported in encrypted JSON file format. A policy file with the same format needs to be imported as per Oracle AVDF release deployed.

6. Enter the **Password**. It is the same password that was set when the Database Firewall policies were exported earlier.
7. Starting in Oracle AVDF 20.9, select an **Action for conflicting policy**. This will determine how imported policies and sets will interact with existing global user, sensitive object, and global sets from Global Sets/Data Discovery. Options include:
   - **Create new policy ensuring the global set names are unique**: Creates a new policy and any global imported set names will be unique.
   - **Create new policy and keep all sets local**: Creates a new policy and all imported sets will be local to this new policy.
   - **Replace the existing policy and the policy sets**: Replace any existing policies and sets with the same name with those that are being imported.

   Sets of database users and database objects can be global or local sets. Global sets can be viewed in and applied to multiple database firewall policies, whereas local sets can only be viewed in and applied to the database firewall policies they were created in. Global sets can be created in Managing Global Sets/Data Discovery.
8. Click **Save**.
   A confirmation message of the import process is displayed. The **User-defined Database Firewall** policies are imported. The policy details are copied to the Audit Vault Server instance and the policies are published. In case there is a name conflict with any of the policies, then a sequence number is added to differentiate. The Audit Vault Server also checks for the file format, validates the JSON file, fields, and values. In case of any issues, an error message is displayed.

   The import process is a background job. The status of the job is displayed in the **Jobs** dialog. The name of the job is `DBFW Policy Import`.
9. The newly imported policy appears in the list. The **Imported** column specifies whether the policy was imported or not. Make any changes to the policy and save them accordingly. The imported policies are published by default, and can be deployed to the Database Firewall. In case there are any further changes required, they can be published again after modification.

> **Note:**
>
> In case the Database Firewall policy has SQL cluster sets and the pertaining SQL statements are not already captured in the Audit Vault Server, then the SQL traffic details are not displayed when the auditor drills down in the cluster for troubleshooting.

7.8.3 Importing Oracle AVDF 20.7 Database Firewall Policies Through CLI

Learn when to use the CLI functionality to import Database Firewall policies.

Oracle AVDF release 20.7 supports export of **User-defined** Database Firewall policies in a `.zip` format. Starting with Oracle AVDF release 20.8, Database Firewall policies are exported into a file in `JSON` format. A policy file with the same format needs to be imported as per Oracle AVDF release deployed. To import the Database Firewall policy files in `.zip` format, a new CLI utility is introduced.

Prerequisites
Follow these steps to complete some prerequisites:

1. The Database Firewall policy file exported in Oracle AVDF release 20.7 is in `.zip` format. Copy this Database Firewall policy `.zip` file to the Audit Vault Server appliance.
2. Log in to the Audit Vault Server through SSH.
3. Run the following command to switch user to *root*:

   ```
   su root
   ```

4. Make sure the `oracle` user has read access to the copied Database Firewall policy .zip file.
5. Unlock *avsys* user by following the next steps.
6. Run the following command to switch user to *dvaccountmgr*:

   ```
   su dvaccountmgr
   ```

7. Run the following command:

   ```
   sqlplus /
   ```

8. Run the following command:

   ```
   alter user avsys identified by <pwd> profile default account unlock;
   ```

> **Note:**
>
> The CLI utility must be run as *oracle* user.

Follow these steps to import the Database Firewall policies using the CLI functionality:

1. Log in to the Audit Vault Server console through SSH.
2. Run the following command to switch user to *root*:

   ```
   su root
   ```

3. Run the following command to switch user to *oracle*:

   ```
   su oracle
   ```

4. Run the following command:

   ```
   /opt/avdf/bin/import_dbfw_policy_zip <policy_zipfile_path>
   ```

5. Enter the password of the policy `.zip` file when prompted.
6. Enter the password of *avsys* user when prompted. Additionally, to seek help while using the CLI, run the following command:

   ```
   opt/avdf/bin/import_dbfw_policy_zip -h
   ```

7. The following message is displayed if the Database Firewall policy file is successfully imported:

```
Request to import DBFW Policy submitted successfully
```

> **Note:**
>
> In case of any error, an appropriate error message is displayed on the screen.

8. The import process is a background job. The status of the import job can be checked in the Audit Vault Server console.

   Click **Settings** tab. The status of the job is displayed in the **Jobs** dialog. The Job Type is `DBFW Policy Import`.

9. After completing the import, run the following to lock the `avsys` user

   a. Run the following command to switch back to root user

      ```
      exit
      ```

   b. Run the following command to switch user to `dvaccountmgr`

      ```
      su dvaccountmgr
      ```

   c. Run the following command

      ```
      sqlplus /
      ```

   d. Run the following command

      ```
      alter user avsys account lock;
      ```

   e. Run the following command

      ```
      exit
      ```

7.9 Copying a Database Firewall Policy

Learn how to copy an existing Database Firewall policy, and edit the same to create a new policy.

1. Log in to the Audit Vault Server console as an *auditor*.
2. Click the **Policies** tab.
3. Click **Database Firewall Policies** tab in the left navigation menu. This page lists the policies you have created, as well as the pre-defined policies.
4. Select the check box against the policy you want to copy.
5. Click **Copy**.

   The **Copy Policy** dialog appears. The **Target Type** field is already filled in.
6. Enter a **Policy Name**.
7. Optionally enter the **Description**.
8. Click **Copy**.

   `Policy created successfully` message is displayed.

9. Click on the name of the policy created to make any further changes.

7.10 Editing a Database Firewall Policy

Learn how to edit a Database Firewall policy.

You can edit Database Firewall policies that you have created or copied, and those policies that are not deployed. After a Database Firewall policy is deployed on the target, it cannot be edited. However, you can copy the policy, redefine with a new name, publish it, and then assign the same to the targets.

1. Log in to the Audit Vault Server console as an *auditor*.
2. Click the **Policies** tab.
3. Click on **Database Firewall Policies** tab in the left navigation menu.
4. Click the name of the specific policy. The details of the policy are displayed in the main page.
5. Edit the policy as required.
6. The rules are categorized under **Session Context**, **SQL Statement**, **Database Objects**, and **Default**. You can make changes to these rules.
7. You can add, edit, or delete a rule. The **Default** rule can only be edited.
8. Starting with Oracle AVDF 20.4, the evaluation order of the rules can be changed (except for **Default**). Follow these steps:
    a. Click **Evaluation Order** button. A dialog appears.
    b. Change the order of the rules using the up or down arrows on the right.
    c. Click **Save**. A confirmation message is displayed on the screen. The updated order of the rules is refreshed on the main page.
9. After making all the changes to the Database Firewall policy, click **Save** in the policy overview page.

7.11 Database Firewall Policy for Capturing Return Row Count

Learn to capture return number of rows for `SELECT` queries.

Starting Oracle AVDF 20.3, if a Database Firewall is deployed in a Monitoring/Blocking (Proxy) or Monitoring (Host Monitor) deployment mode, it can capture the returned number of rows for `SELECT` SQL statements. If deployed in Monitoring/Blocking (Proxy) mode this requires no additional configuration, but if deployed in Monitoring (Host Monitor) mode, you need to enable it to capture database responses. See Enabling Database Response Monitoring in the *Oracle AVDF Administrator's Guide* for more information. The details for the returned number of rows are displayed in **All Activity** and **Database Firewall Reports** under the column **Row Count**. This field can be used in Alert policies to detect attempts to retrieve more than expected amount of data.

The field **Capture number of rows returned for SELECT queries** is available in the Audit Vault Server console when defining the **Database Object** rule of the Database Firewall policy. It is available when the target type is an Oracle Database and when **Data Manipulation Readonly** is selected in the **Statement Classes** field. **Data Manipulation Readonly** field is replaced with **Select** in Oracle AVDF 20.4 and later. When this option is enabled, the Database Firewall captures the returned number of rows for `SELECT` queries.

Step	Process	Reference
1	Configuring Database Firewall policy to capture return row count	Database Object Rule
2	Configuring alert policy based on row count	Writing an Alert Condition
3	Viewing row count in reports	All Activity Reports Database Firewall Reports

7.12 Configuring Firewall Policy for SQL Statements

Learn about policies that can be used for SQL traffic to the database.

Database Firewall is a multistage firewall that monitors SQL traffic going into the database and determines with high precision whether to allow, log, alert, substitute, or block the SQL statements. The SQL traffic goes through multiple stages that checks for the IP address, database or OS user, program name, SQL statement category, such as DDL and DML, and database tables being accessed. It blocks and alerts block listed SQL and SQL that is not in the allowed list or SQL statements. This prevents SQL injection attacks by providing an option to configure policy rules based on allowed list of SQL requests from trusted application paths.

Successful SQL statement monitoring using Database Firewall depends on deciding an effective firewall policy and selecting the appropriate firewall deployment.

7.13 Blocking SQL and Creating Substitute Statements

Learn how to block a SQL statement and provide a sample SQL statement as a substitute.

Database Firewall can block SQL statements when deployed in **Monitoring / Blocking (Proxy)** mode. Database Firewall can block a SQL statement and you can provide a sample SQL statement as a substitute. A substitute statement may be necessary to ensure that the database client is presented with an appropriate message when a statement is blocked. This substitute statement may also be helpful in misleading a malicious user with the sample SQL statement provided. It can also be configured with a threshold value for blocking or alerting.

Substitute statements cannot be applied on the following SQL commands:

- `LOGIN USERNAME`
- `EXECUTE CURSOR`
- `ENCRYPTED`
- `SHUTDOWN`
- `DESCRIBE`
- `ORADEBUG`
- `TRANSACTION`
- `LOB`
- `INVALID OPERATION`
- `COMMENT`
- `COMPRESSED`

When creating substitute statements, ensure the results can be handled by the client applications. The following is an example of a good substitute statement for Oracle Database target:

```
SELECT 100 FROM DUAL
```

You can block or warn when the SQL statements occur a specified number of times. You can choose to block the SQL statement or produce a warning if a statement repeats a specified number of times (or threshold value) in the selected cluster. You should always enable logging for blocked statements.

7.14 SQL Statement Encrypted with Oracle Native Network Encryption

Learn how Database Firewall can be used to monitor Oracle Database target that uses native network encryption.

When this functionality is enabled, network traffic between the client and database server is encrypted. In order for the Database Firewall to decrypt and apply policy on SQL statements, Oracle AVDF administrator must configure the Database Firewall to decrypt this traffic.

> **See Also:**
>
> Monitor Native Network Encrypted Traffic Through Database Firewall for Oracle Databases

8 Reports

Oracle Audit Vault and Database Firewall provides a set of reports that you can generate and customize.

8.1 About the Reports in Audit Vault and Database Firewall

The Oracle Audit Vault and Database Firewall reports are automatically generated reports on collected audit and network event data from targets and from Database Firewall data.

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 activity reports, summary reports, compliance reports, assessment reports, alert reports, and user-defined 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 target database, you can add the target to the appropriate group (such as the SOX group) from the **Targets** tab.

In Oracle AVDF 20.1-20.12, auditors can view and customize reports generated by super auditors as long as they have access to the target.

Starting in Oracle AVDF 20.13, only super auditors will be able to view and customize reports generated by a super auditor.

However, an auditor can 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.

> **Note:**
>
> Reports run faster if the audit data is in memory on the Audit Vault Server. If your Oracle Audit Vault and Database Firewall administrator has enabled Oracle Database In-Memory, you will see a date range in the top right corner of the Home tab. Reports for the specified date range run faster. See how to enable in memory at Enabling Oracle Database In-Memory for the Audit Vault Server.

See Also:

- Creating and Modifying Target Groups
- Creating or Modifying an Email Template

8.2 Activity Reports

Activity reports capture information such as alerts or changes to stored procedures.

8.2.1 About the Activity Reports

Activity reports cover entitlement data, operating system correlation data, alerts, and other information.

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

- Activity Reports
- Entitlement Reports
- OS Correlation Reports
- Database Firewall Reports
- Stored Procedure Changes Reports (Stored Procedure Audit Reports if prior to AVDF 20.1)
- DB Vault Activity
- SQL Firewall Violations Report (Starting in Oracle AVDF 20.14)

See Also:

Managing and Viewing Entitlement Data

8.2.2 Activity Reports

Learn about activity reports.

Note:

The maximum limit for the `ROW_LIMIT` parameter is `20000`. Use additional filters available to view specific audit events in the report.

8.2.2.1 About the Activity Reports

Any auditor can access the activity reports.

You can access Activity Reports from the **Reports** tab, and then by clicking **Activity Reports** tab in the left navigation menu. In the main page expand the **Activity Reports** section.

The default activity reports track general database access activities such as all activity, data access activities, user login/logout activities, and entitlements.

> **Note:**
>
> - The **Client Host** (host name of the client) value is displayed in the reports only if the DNS is configured for the Audit Vault Server.
> - The **Event Status** value in the reports is displayed only if Database Response Monitoring is enabled for the respective monitoring point.

8.2.2.2 Activity Overview Report

The Activity Overview Report captures information about all monitored and audited events. It has been deprecated in AVDF 20.1.

The **Activity Overview** can be viewed from **Saved Reports** tab in the left navigation menu. The **Activity Overview** page provides a summary of all audited and monitored 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 Audit Vault and Database Firewall 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 Audit Vault and Database Firewall administrator to check the server-side log files (alert and trace logs) for errors. If there are errors, then contact Oracle Support.

> **Note:**
>
> Apply filters based on date and time. Access the audit interactive reports. For example, **Activity Overview** report. Click on **Actions**, and then select **Filter**. Choose `Row` as the **Filter Type**.
>
> In the **Filter Expression** field, enter the query as follows:
>
> ```
> <event_time> BETWEEN ‘MM/DD/YYYY HH:MM:SS PM/AM’ and ‘MM/DD/YYYY HH:MM:SS
> PM/AM’
> ```
>
> For example:
>
> ```
> BZ BETWEEN ‘8/20/2018 2:30:50 PM’ and ‘8/20/2018 2:40:50 PM’
> ```

Related Topics

- Behavior Changes, Deprecation, and Desupport Notices in Oracle Audit Vault and Database Firewall 20.1

8.2.2.3 All Activity Report

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

Starting in Oracle AVDF 20.11, users can add filters in the UI interactive report and copy them to the alert condition.

1. Navigate to the **Activity Reports - All Activity** page.
2. Filter the report as desired.
3. Click on **Create as alert policy**.
   The **Create Alert** page will appear with the **Condition** field automatically filled with the filters you created on the report. See Creating or Modifying an Alert for more information.

Related Topics

- Filtering by a Global Set in an All Activity Report
  Learn about applying a Global Set filter on an All Activity Report.

8.2.2.4 All Activity by Privileged Users

The **All Activity by Privileged Users** report displays details of observed activity of privileged users targeting audit policy for a specified period of time.

8.2.2.5 Data Access Report

The **Data Access** report displays details of read access events.

For example: SELECT, read access to data events.

> **See Also:**
>
> Related Event Data Appendices for related data access audit events in a specific target type

8.2.2.6 Audit Policy Activity Report

The **Audit Settings** report (known as **Audit Policy Activity** report in Oracle AVDF 20.4 and later) is available under the **Database Settings** category.

It displays details of observed user activity targeting audit settings for a specified period of time.

8.2.2.7 Data Modification Report

The **Data Modification** report displays events that lead to data modification.

For example: DML activities (insert, update, and delete).

8.2.2.8 Data Modification Before-After Values Report

The **Data Modification Before-After Values** report displays before and after values of modified data in Oracle Database or Microsoft SQL Server.

Data for this report comes from the `TRANSACTION LOG` audit trails that are written by databases. An administrator must configure and start a `TRANSACTION LOG` audit trail for the target to be monitored. The location for the `TRANSACTION LOG` audit trail should be the Oracle Golden Gate Integrated Extract directory. See Transaction Log Audit Data Collection Reference for more information.

Starting with Oracle AVDF 20.10, the **Data Modification Before-After Values** report displays the key columns for an update operation, along with the modified column and its old and new values. The **Primary Key-Value(s)** column contains the values of the table's key columns. You can use these values to uniquely identify a modified record in the table. By default, key columns contain the values of the primary keys. If needed, you can configure any column as a key column in the Golden Gate parameter file.

You can filter the **Data Modification Before-After Values** report. To apply the filter on a **Column Name**, **Before Value**, and **After Value**, select `Like` as the **Operator**.

Note:

- The Transaction Log collector can read the Golden Gate Integrated Extract files that contain the before and after records. Oracle GoldenGate must be configured to generate the Integrated Extract in the `XML_AUDIT_VAULT` XML format.
- To check the change in a column value of a particular table, add filter on **Target Object**. The filter can be something like **Target Object** Equal to (=) table name and `Column Name` in the **Column** field. For example, if the **Address** column of the employee table is changed, the filter should be **Target Object** = `EMPLOYEE` and **Column Name** like `%ADDRESS%`.
- The session information (Program Name, OS User Name, Client Host Name, OS Terminal, Process ID, Client ID) will always be empty for Microsoft SQL Server and MySQL target, because these targets do not provide the session information to the GoldenGate Extract.
- The Command Text field will be populated by Transaction Log audit trail only for DDL operations but will always be empty for DML operations. You have to configure `UNIFIED_AUDIT_TRAIL TABLE` trail for Oracle target or `sqlaudit DIRECTORY` trail for Microsoft SQL Server target to get the Command Text for DML operations.

8.2.2.9 Database Schema Activity Report

The **Database Schema** report (known as **Database Schema Activity** report in Oracle AVDF 20.4 and later) is available under **Database Settings** category.

It displays information about changes in the database schema. For example: DDL commands (alter session).

8.2.2.10 Entitlement Activity Report

The **Entitlements Report** (known as **Entitlement Activity** report in Oracle AVDF 20.4 and later) is available under **Entitlement Reports** category.

It displays information about changes in grants of database privileges and roles. For example: DCL commands (GRANT access, revoke).

8.2.2.11 Failed Login Events Report

The **Failed Login Events** report displays information about failed authentication attempts.

8.2.2.12 Login and Logout Report

The **Login and Logout** report displays information about all successful login and logout events.

8.2.2.13 Startup and Shutdown Report

The **Startup and Shutdown** report displays details of observed targets startup and shutdown events for a specified period of time.

8.2.3 Entitlement Reports

The **Entitlement Reports** capture information such as a user's roles, object privileges, system privileges, and so on.

> **See Also:**
>
> Entitlement Report Descriptions

8.2.4 OS Correlation Reports

The **OS Correlation Reports** provide useful information about operating system related activities that users perform.

The **Linux SU SUDO Transition** report provides details of database events that are correlated with the Linux operating system user before `su` or `sudo` transition. It is specific to Oracle Database targets running on Linux. This report uses the OS and Database audit trails to correlate `su` and `sudo` activity on the Linux OS with Oracle Database audit events. This lets auditors see the original OS user in cases where this user runs a shell or executes a command as another user by using `su` or `sudo`.

For example, suppose the Linux OS user, `user_01`, logs in to a Linux terminal, and then performs `su` or `sudo` activity to another Linux user, `user_02`. Then `user_01` connects as the Oracle Database user `user_db` locally and then remotely, and performs some database activities.The Linux SU SUDO Transition report displays the Oracle Database audit events with the additional columns `OS User Transition`, `Transition Type`, and `Database Connection`

Type. These columns provide information about the correlation that occurred before the Oracle Database operations. For example:

Column Name	Data
OS User Transition	user_01 > user_02
Transition Type	su *(for a sudo operation, it would list sudo)*
Database Connection Type	Local *(for a remote database connection, it would be remote)*
Database User Name	user_db

Similarly, the Linux SU SUDO Transition Report displays data for local and remote database connections and for SYS and non-SYS users.

In order to generate information for this report, you must have audit trails configured and running for both the Oracle Database and for the Linux OS on which the database runs. The Linux OS audit trail must be registered with a host name, and not an IP address. See *Oracle Audit Vault and Database Firewall Administrator's Guide* for instructions on how to configure audit trails in Oracle AVDF.

Be aware that if there is a slippage in Linux events, then the report does not show the correct correlation data.

Table 8-1 shows the currently available correlation reports.

Table 8-1 su/sudo Correlation Reports

Report	Description
Linux SU SUDO Transition	Details of database events correlated with the Linux operating system user before su or sudo transition

8.2.5 Database Firewall Reports

The **Database Firewall Reports** contain data that is collected if a target is monitored by the Database Firewall (using a firewall policy).

Data displayed as part of the reports include:

- **Threat Severity**
- **Target**
- **User**
- **OS User** (Only in the Monitored Activity by OS User report)
- **Client Host**
- **Client Program**
- **Event**
- **Object**
- **Event Status**
- **Event Time**

Note:

- The **Client Host** (host name of the client) value is displayed in the reports only if the DNS is configured for the Audit Vault Server.
- The **Event Status** value in the reports is displayed only if Database Response Monitoring is enabled for the respective monitoring point.

Table 8-2 lists the Database Firewall reports.

Table 8-2 Database Firewall Reports

Report Name in Oracle AVDF 20.4 and Earlier	Report Name in Oracle AVDF 20.5 and Later	Description
Database Firewall Monitored Activity	Monitored Activity	SQL activity monitored by Database Firewall.
Blocked Statements	Blocked Activity	SQL activity blocked by Database Firewall.
Database Traffic Analysis by OS User	Monitored Activity by OS User	SQL activity monitored by Database Firewall grouped by OS user.
Invalid Statements	Invalid Activity	SQL activity not recognized by Database Firewall.
Warned Statements	Alert Activity	SQL activity marked as warning by Database Firewall.

8.2.6 Stored Procedure Changes

The **Stored Procedure Changes** auditing reports allow you to audit changes to stored procedures on target databases.

You can access **Stored Procedure Changes** reports from the **Reports** tab, and then by clicking **Activity Reports** in the left navigation menu. The **Stored Procedure Changes** reports is displayed in the list of reports on the main page.

Oracle Audit Vault and Database Firewall connects to the target database at scheduled intervals and discovers any changes or additions that have been made to stored procedures.

Table 8-3 lists the Stored Procedure Auditing reports.

Table 8-3 Stored Procedure Changes Report

Report	Description
Created Stored Procedures	Creation history of stored procedures
Stored Procedure Modification History	Modifications of stored procedures
Deleted Stored Procedures	Deletion history of stored procedures

8.2.7 DB Vault Activity

If your Oracle Database targets have Database Vault enabled, then the **Database Vault Activity** report shows the details of Oracle Database Vault activity.

This report captures activities such as Database Vault events that capture policy or rule violations, unauthorized access attempts, and so on.

Oracle Database Vault may be enabled in an Oracle Database target to provide greater security by restricting access to sensitive areas of the database. For example, you can restrict administrative access to employee salaries, customer medical records, or other sensitive information.

You can check if Oracle Database Vault is enabled in a target by running the following SQL query in SQL*Plus:

```
SELECT PARAMETER, VALUE FROM V$OPTION WHERE PARAMETER = 'Oracle Database Vault';
```

Remember that the `PARAMETER` column value is case sensitive.

If Oracle Database Vault is enabled, the following output appears:

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

8.2.8 SQL Firewall Violations Report

Starting in Oracle AVDF 20.14, the **SQL Firewall Violations Report** contains data that is collected if a SQL statement or session context violates your established SQL Firewall policies. This information is collected from the `SYS.DBA_SQL_FIREWALL_VIOLATIONS` audit trail.

Data displayed as part of the reports include:

- **Target**
- **User**
- **Client Program**
- **Event**
- **Object**
- **Event Time**

Related Topics

- Using SQL Firewall with AVDF
- DBA_SQL_FIREWALL_VIOLATIONS

8.2.9 Alert Reports

The alert reports track critical and warning alerts. The alerts report will only show alerts from the past three months, as alerts have a retention policy of three months online and zero months in archive.

Alert reports can be accessed from the **Alerts** tab, and then the **Alerts** tab in the left navigation menu.

> **Note:**
>
> Starting with 20.1 the alerts reports are accessed from the **Alerts** tab instead of from the **Reports** tab.

Alternatively, you can view the **All Alerts** report from the **Reports** tab and the **Generated Reports** tab on the left navigation menu. Enable the filter for the **All Alerts** report name above the table. Click the **All Alerts** name to download the report.

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

There are two alert severities:

- **Critical Alerts** - This report shows critical alerts that were raised by Audit Vault Server.
- **Warning Alerts** - This report shows warning alerts that were raised by Audit Vault Server.

Related Topics

- Creating Alerts and Writing Alert Conditions
  Learn about creating alerts and writing alert conditions.
- Responding to an Alert
  After you have created alerts and when they are generated, you or other auditors can respond to them.

8.3 Summary Reports

Learn about Summary Reports.

8.3.1 Trend Charts Report

The Trend Charts Report shows the event trends (total events) in the last *n* days.

Table 8-4 shows the available event trend reports.

Table 8-4 Trend Charts

Report	Description
Event Trend	Trend of all events
Event Trend By Target	Trend of events by target
Event Trend By Client IP	Trend of events by client IP
Event Trend By OS User	Trend of events by OS user

8.3.2 Anomaly Reports

Anomaly reports show new and dormant user and client IP anomalies (total anomalies) in the last *n* days.

Anomaly reports don't require any configuration to display data in the reports.

Table 8-5 shows the available anomaly reports.

Table 8-5 Anomaly Reports

Report	Description
New or Dormant User Activity	Activity by newly created or dormant users
New or Dormant Client IP Activity	Activity from newly seen or dormant client IP addresses

8.3.3 All Activity Reports

The All Activity Reports report shows summaries of client and operating system user activities, DDL and DML activities, and failed logins.

Table 8-6 shows the available summary reports.

Table 8-6 All Activity Reports

Report	Description
Activity Summary by Client IP and OS User	Events grouped by user and client IP
Activity Summary by Target	Events grouped by target
DDL Activity Summary by Target	Schema changes grouped by target
DML Activity Summary by Target	Data modifications grouped by target
Failed Logins Summary by Target	Failed authentication attempts grouped by target

8.4 Compliance Reports

The Compliance Reports capture information to ensure that your system is meeting regulatory compliance standards.

8.4.1 About the Compliance Reports

The compliance reports 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:

- Data Privacy Reports (GDPR)
- Payment Card Industry (PCI)
- UK Data Protection Act (DPA)
- USA Gramm-Leach-Bliley Act (GLBA)
- USA Health Insurance Portability and Accountability Act (HIPAA)
- USA Reports based on IRS Publication 1075
- USA Sarbanes-Oxley Act (SOX)

To access the compliance reports, click the **Reports** tab, and then click on **Compliance Reports** tab in the left navigation menu.

8.4.2 Configuring Compliance Reports

To configure compliance reports, you need to associate one or more targets to the compliance category, such as Data Privacy Report (GDPR).

1. Ensure that the appropriate entitlement data is available for the target.

   See Retrieving User Entitlement Data for Oracle Database Targets for complete information.

2. Log in to the Audit Vault Server console as an auditor.
3. Click the **Reports** tab.
4. Click **Compliance Reports** in the left navigation menu.
5. Select a category from the **Compliance Reports Category** drop-down list.

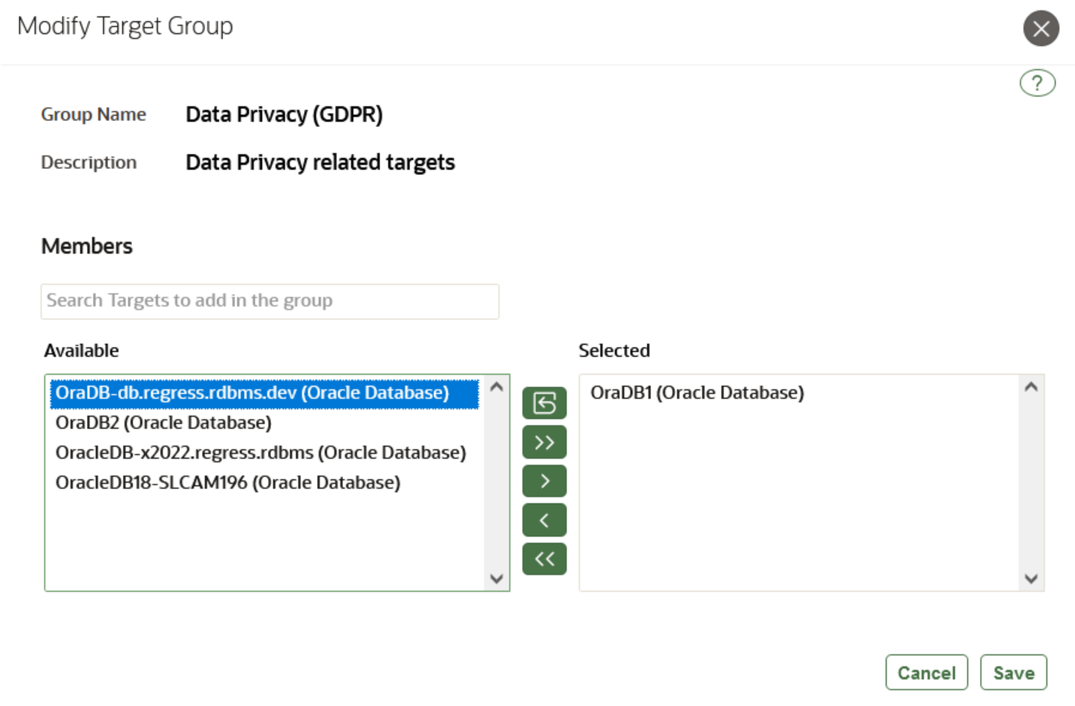
   The list of reports on this page changes depending on which category you select.

6. Click the **Go** button to associate targets with the selected compliance reports category.
7. In the **Modify Target Group** dialog box, move the targets that you want to associate with the compliance category from the **Available** column to the **Selected** column.

   To select multiple targets, press and hold the Ctrl key as you click each target.

   To move the selected targets, click the **Move (>)** or **Move All (>>)** button.

   The following screen shot shows an example of the **Modify Target Group** dialog box. There are five total targets. One target has been moved to the **Selected** column and the **Available** column lists the remaining four targets.



Modify Target Group

Group Name: Data Privacy (GDPR)

Description: Data Privacy related targets

Members

Search Targets to add in the group

Available:
- OraDB-db.regress.rdbms.dev (Oracle Database)
- OraDB2 (Oracle Database)
- OracleDB-x2022.regress.rdbms (Oracle Database)
- OracleDB18-SLCAM196 (Oracle Database)

Selected:
- OraDB1 (Oracle Database)

8. Click **Save**.
9. On the **Compliance Reports** page, select the category from the **Compliance Reports Category** drop-down list again.
10. Schedule or generate the necessary reports.

    See Scheduling and Generating PDF or XLS Reports.

Related Topics

- Filtering on Sensitive Objects in Compliance GDPR Reports

8.4.3 Data Privacy Reports

Learn about the Data Privacy Reports.

8.4.3.1 About Data Privacy Reports

Data privacy is also known as information privacy or data protection.

It is concerned with the relationship between collection and dissemination of data and technology, the public perception, expectation of privacy, the legal regulation, and political issues surrounding that data. The details and implementation of data protection vary depending on the region, the context, the methods, and the extent to which it is regulated.

GDPR (General Data Protection Regulation) is a regulation in European Union (EU) law on data protection and privacy for all individuals within the European Union. It addresses the export of personal data outside the EU. GDPR is an overhaul of the existing European Commission data protection legislation. It harmonizes data privacy laws, aims to strengthen, and unify these laws for EU citizens. GDPR is about individuals having autonomy and control over their data. It primarily aims to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. It is important for organizations to protect information they possess about individuals to prevent others from accessing or misusing their personal information.

GDPR is applicable in case the following are based in the European Union:

- Data controller
- Data processor
- Data subject or the person
- Data recipient
- Authority supervising and auditing data
- An organization that collects data from EU residents
- An organization that processes data on behalf of data controller like the service providers
- An organization based outside the EU that collects or processes personal data of individuals located inside the EU

According to the European Commission, *personal data* is any information relating to an individual. This information can be private, professional, or public life of the individual. It includes, but is not limited to, a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or an IP address.

In order to comply with GDPR, the data controller must implement measures, which meet the principles of data protection by design, and data protection by default. It is the responsibility and the liability of the data controller to implement effective measures and to demonstrate the compliance of processing activities. This includes if the processing is performed by an external data processor on behalf of the controller.

GDPR considers encryption as one of the components in the security strategy, and mandates that organizations need to consider assessment, preventive, and detective controls based upon the sensitivity of the personal data in their possession.

Articles 30 and 33 of GDPR, mandate that organizations must maintain a record of its processing activities. This can only be achieved by constantly monitoring and auditing activities on personal data. This data can be used to timely notify authorities in case of a breach. In addition to mandating auditing and timely alerts, GDPR also requires that organizations must keep the audit records under their control. A centralized control of audit records prevents attackers or malicious users to cover the tracks of their suspicious activity by deleting the local audit records. There are four reports under Data Protection. They primarily focus on access to sensitive data by regular or privileged users and also privilege settings on objects.

8.4.3.2 Importing Sensitive Data Into Repository

Information about sensitive data is imported and stored in the Oracle AVDF repository.

You can import a data file in `.csv` and `.xml` format. These data files are sourced from Oracle Enterprise Manager and Oracle Database Security Assessment Tool by running data discovery job to search for sensitive data in specific Oracle Database targets.

Oracle Database Security Assessment Tool generates the file in `.csv` format and Oracle Enterprise Manager generates the file in `.xml` format. The data file extracted contains a list of sensitive columns that is imported into the repository. It is viewed in the Audit Vault Server GUI using **Data Privacy Reports**.

> **Note:**
>
> Oracle AVDF 20 supports Oracle Enterprise Manager Cloud Control versions 13.4 and later.

> **See Also:**
>
> - *Oracle Enterprise Manager Lifecycle Management Administrator's Guide* to run data discovery job and search for sensitive data for specific targets using *Oracle Enterprise Manager*.
> - *Oracle Database Security Assessment Tool User Guide* to run a discovery job using *Oracle Database Security Assessment Tool*.
> - Oracle Data Masking and Subsetting Guide for more information on Application Data Modeling that stores the list of applications, tables, and relationships between table columns and maintains sensitive data types.

1. Ensure you have the sensitive data report in `.csv` or `.xml` format by running data discovery job through *Oracle Database Security Assessment Tool* or *Oracle Enterprise Manager* respectively.
2. Save the file in your local drive.

3. Log in to the Audit Vault Server terminal as *root* user.
4. Switch to *oracle* user, by running the following command:

   ```
   su - oracle
   ```

5. Run the following commands to grant (or revoke) *av_sensitive* role to the *admin* user, or list of *admin* users.

   For Oracle AVDF 20.5 and Later

Action	Command
To grant *av_sensitive* role to the *admin* user.	`/usr/local/dbfw/bin/av_sensitive_role.py grant <admin1> <admin2>`
To revoke *av_sensitive* role from the *admin* user.	`/usr/local/dbfw/bin/av_sensitive_role.py revoke <admin1> <admin2>`

   For Oracle AVDF 20.4 and Earlier

Action	Command
To grant *av_sensitive* role to the *admin* user.	`/usr/local/dbfw/bin/av_sensitive_role grant <admin1> <admin2>`
To revoke *av_sensitive* role from the *admin* user.	`/usr/local/dbfw/bin/av_sensitive_role revoke <admin1> <admin2>`

6. Log in to the Audit Vault Server console as *admin* user.
7. Click on **Targets** tab. The **Targets** sub tab in the left navigation menu is selected by default. The main page lists the configured targets to which you have access. You can sort or filter the list of targets.
8. Click the name of a specific target.

   The specific target page is displayed.
9. Click **Sensitive Objects** button in the top right corner.
10. Click **Browse** against the **Import From (.xml / .csv)** field. Choose the sensitive data file saved in your local drive.

    > **See Also:**
    >
    > - *Oracle Enterprise Manager Lifecycle Management Administrator's Guide*
    > - *Oracle Database Security Assessment Tool User Guide*
    > - Oracle Data Masking and Subsetting Guide
    > - Download Oracle Database Security Assessment Tool

11. Click **Upload**.

Result:

A pop up message `File loaded successfully` is displayed on the screen. The recent target file upload information is displayed on the GUI. The previous one is overwritten.

12. Click **Save**.

> **Note:**
>
> - In case the user does not have the required role to import the sensitive data, or if the uploaded file is in incorrect format, then appropriate error message is displayed.
> - The report contains sensitive data generated from the recent `.csv` or `.xml` file uploaded. The earlier imported sensitive data is overwritten and the history is not maintained.

8.4.3.3 Accessing Data Privacy Reports

After the sensitive data file is imported into the repository, you need to associate one or more targets with the data privacy reports before you can schedule or generate the reports.

Use the Audit Vault Server console to configure and view the data privacy reports.

1. Associate at least one target with the data privacy reports.

   See Configuring Compliance Reports for instructions.

2. Schedule or generate the data privacy reports.

   See Scheduling and Generating PDF or XLS Reports.

You can view the following data privacy reports:

Report	Description
Sensitive Data	Displays details about sensitive data like the schema name, target, column name, sensitive type, object, and sensitive objects set.
Access Rights to Sensitive Data	Displays details about users' access rights to sensitive data. Use this report to view the privileges that are granted to users on sensitive data. See the example report that appears after this table. The user may have one or more of the privileges that are listed in the **Privileges** column for the respective sensitive data. The user can have these privileges assigned directly or through roles that have been granted. Privileges that have been granted to sensitive data that is assigned to a role are displayed only when the role is assigned to any user. Privileges on sensitive data may be granted to the user group `PUBLIC`. In this case, the privilege is granted to all users. The privilege that's granted to `PUBLIC` is not visible in the report. The report contains only privileges on sensitive data that are granted as object privileges. System privileges are not displayed in the report.
Activity on Sensitive Data	Displays details about activity on sensitive data by all users.

Report	Description
Activity on Sensitive Data by Privileged Users	Displays details about activity on sensitive data by privileged users.

Example 8-1 Access Rights to Sensitive Data Report

Target Name : <Target Name 1>

Sensitive Object	User Name	Privileges
`Table_1`	User X	`DELETE,INSERT,SELECT,UPDATE`
`Table_2`	User Y	`DELETE,INSERT,SELECT,UPDATE`
`Table_3`	User Z	`DELETE,INSERT,SELECT,UPDATE`

8.4.3.4 Implementation In Oracle Audit Vault And Database Firewall

Oracle Audit Vault and Database Firewall complies with data protection directives and regulations by offering special services.

These services include centralized auditing, monitoring, reporting, and alerting of anomalous activity on the database. It reports any access to sensitive data stored in the database.

The report relates to sensitive data, as identified and received from the sensitive data discovery processes. It contains information regarding activity on sensitive data by all users including privileged users.

Oracle Audit Vault and Database Firewall complies with data protection at source by centralizing control and administration. It stores and manages the data for processing in a centralized location. It monitors and sends timely alerts of suspicious behavior. It can centrally manage millions of audit records, or different types of security policies, by simplifying the administration related tasks. This is managed using Oracle Enterprise Manager that has a unified web based GUI.

Oracle Audit Vault and Database Firewall centrally collects and manages audit records. It monitors, alerts, reports, and blocks suspicious behavior.

> **Note:**
>
> Oracle Audit Vault and Database Firewall helps in complying with data privacy regulations such as GDPR.

8.5 Assessment Reports

The assessment reports capture security assessment data from Oracle Databases that are configured as targets in Oracle Audit Vault and Database Firewall (Oracle AVDF) 20.9 and later.

8.5.1 About Assessment Reports

Assessment reports provide information and recommendations that are helpful in securing your Oracle Database system.

These recommendations reflect best practices for database security and should be part of any strategy for Data Protection by Design and by Default. Technical controls alone are not sufficient for compliance. Passing all findings does not guarantee compliance.

Oracle Audit Vault and Database Firewall does not check all controls covered by the DISA STIG. Findings mapping to DISA STIG focus on technical controls. Process-related controls require manual evaluation.

The report provides a view of the current status. The results shown are provided for informational purposes only and should not be used as a substitute for a thorough analysis or interpreted to contain any legal or regulatory advice or guidance.

You are solely responsible for your system and the data and information gathered during the production of this report. You are also solely responsible for the execution of software to produce this report and for the effect and results of the execution of any mitigating actions identified herein.

Oracle provides this analysis on an "as is" basis without warranty of any kind and Oracle hereby disclaims all warranties and conditions whether express, implied, or statutory.

> **Note:**
>
> Assessment reports will be purged after 18 months from the time of data retrieval.

8.5.2 Setting a Baseline for Security Assessment Reports

Starting in Oracle AVDF 20.10, you can view security assessment drift reports that compare the latest assessment to either the baseline or a previous assessment. The baseline is a user-designated security assessment report that represents a good security posture for your database(s).

1. Click the **Reports** tab.
2. Click **Assessment Reports** in the left navigation.
3. Click on the **Detailed Report**.
4. Select either all targets or a specific target from the **Target** drop down.
5. Select a security assessment based on the time it was run from the **assessed time** drop down.
6. Click **Set As Baseline**.

8.5.3 Viewing Assessment Reports

To access the assessment reports, click the **Reports** tab and then click **Assessment Reports** in the left navigation menu.

Select the type of report that you want to view. Within each report, you can drill down to detailed reports that list all targets and assessments that are filtered to meet the criteria for the report. From there, click the **Report View** icon to see the details for each finding.

You can also perform all standard Oracle AVDF report operations, such as scheduling reports, viewing previously generated reports, filtering, and downloading reports.

For descriptions of the severity levels, see Severity Levels.

For a list of the categories and assessments, see Categories and Assessments.

For details about using each report, see the following tables.

Security Assessment Reports

Report Name	Usage
Summary by Target	Use this report to see the number of assessment within each severity for each target. For example, for each target, it gives the number of assessments that are high risk, medium risk, and so on. Click a target in the report to see the results of all assessments for that target, including assessments that passed. You can also see if a target has not been assessed. In this case, click the target name link to go to the Schedule Retrieval Jobs page, where you can submit the security assessment retrieval job. See Retrieving Security Assessment Data for Oracle Database Targets.
Summary by Severity	Use this report to see the number of targets and assessments within each category for each severity. For example, for the high risk severity level you can see the number of targets and the number of assessments within the User Accounts category. Click a severity level in the report to see a detailed list of all targets and assessments that have that severity.
Summary by Category	Use this report to see the number of targets with assessments within each category and assessment description. For example, for the User Accounts category you can see the number of targets with the Inactive Users assessment description. Click the number in the **Number of Targets** column to see a detailed list of targets and findings for the corresponding assessment. The detailed list is automatically filtered to hide assessments that passed, but you can remove that filter to see all assessment findings.
Summary by Feature Utilization	Use this report to see the number of targets that are using each security feature within each category. For example, 1 in the Unified Auditing feature of the Auditing category means that one target is using that feature. You can also see the number of targets that don't use a security feature and the number of targets for which the feature isn't available. Click the number in the **Utilized**, **Not Utilized**, or **Not Available** column to see a detailed list of targets that fit that description and the findings for the corresponding category of security features.

Report Name	Usage
Detailed Report	See all findings for all targets, categories, and severity risk levels. You can filter the list to show specific criteria. **Note:** Starting in Oracle AVDF 20.10 only the first 32,767 characters will be shown in the Excel report.
Exception Report	Shows the exceptions added for security assessment reports of all Oracle Database targets.

Security Assessment Compliance Reports

These reports display the Security Assessment Detailed Report with filters applied for the selected compliance type.

Report Name	Usage
Oracle Best Practices Report	For all targets, see the results of all assessments that relate to Oracle best practices.
STIG Report	For all targets, see the results of all assessments that relate to Security Technical Implementation Guide (STIG) guidelines from the Defense Information Systems Agency (DISA). Click the **Report View** icon to find references to the specific STIG guidelines. **Note:** Starting in Oracle AVDF 20.10 only the first 32,767 characters will be shown in the Excel report.
CIS Report	For all targets, see the results of all assessments that relate to Center for Internet Security (CIS) benchmark recommendations. Click the **Report View** icon to find references to the specific CIS recommendations.

Report Name	Usage
GDPR Report	For all targets, see the results of all assessments that relate to European Union General Data Protection Regulation (EU GDPR) guidelines. Click the **Report View** icon to find references to the specific GDPR guidelines. **Note:** Starting in Oracle AVDF 20.10 only the first 32,767 characters will be shown in the Excel report.

Security Assessment Drift Reports

Starting in Oracle AVDF 20.10 these reports show how a selected assessment report differs from the baseline or from a previous assessment report.

Starting in Oracle AVDF 20.11, users can monitor drift report details directly on the Audit Vault Server console **Home** page. If no baseline has been established, the graph will appear empty. Once a baseline is set, hovering over the drift graph will show additional information. Users can also click on the graph to access the complete report. To analyze findings based on security risk levels, it is essential to establish a baseline for the specified targets. This ensures accurate calculation of drift between the baseline and the latest data.

To compare the latest assessment to the baseline, select the **baseline** option and click **Go**.

To compare the latest assessment to a previous assessment, select the **selected timeline** option, type in an integer for how many days, weeks, months, or years prior the assessment was, select the appropriate unit of time, and click **Go**. The oldest security assessment from the designated amount of time will be used in the comparison.

Drift Summary by Target	Use this report to see how the drift, the number of risks added, modified, or removed, within each severity in the latest assessment changed from the baseline or a previous assessment for each target. For example, for the Database1 target you could see that two risks were modified for the high risk severity and that three risks were added for the evaluate severity. Click a target in the report to see a detailed comparison of the latest assessment to the baseline or a previous assessment. From the detailed comparison report you can also see more details about the changes for each row by clicking the Single Row View icon on the left.

Drift Summary by Severity	Use this report to see how the drift, the number of risks added, modified, or removed within each category in the latest assessment changed for each severity from the baseline or a previous assessment. For example, you can see that since the latest assessment one low risk assessment was added in the Auditing category. Click a category in the report to see a detailed comparison of the latest assessment to the baseline or a previous assessment. You can also see more details about the changes for each row by clicking the Single Row View icon on the left.
Drift Summary by Feature Utilization	Use this report to see how the number of targets that are using each security feature within each category changed in the latest assessment from the baseline or a previous assessment. For example, 1(+1) in the Unified Auditing feature of the Auditing category means that one target is using that feature and that this has increased by one from the assessment you are comparing to. Similarly, 1(-1) would indicate that one target is using a feature but that this has decreased by one from the assessment you are comparing to.1(-) indicates that there was no change in the number of targets using that feature. Click the number in the **Utilized** column to see a detailed list of the changes that fit that description and the findings for the corresponding category of security features.
Detailed Drift Report	See a comparison report how all findings in the latest assessment changed from the baseline or a previous assessment for all targets, categories, and severity risk levels. You can filter the list to show specific criteria. You can also see more details about the changes for each row by clicking the Single Row View icon on the left.

8.5.4 Adding Exception for Security Assessment Reports

Starting in Oracle AVDF 20.13, you have the ability to customize how assessments are treated by either updating their severity level or deferring them for a certain period. This feature allows administrators to better align the security posture with specific needs or risk tolerance. Below are the steps and detailed explanations for both actions.

8.5.4.1 Updating the Severity of an Assessment

In Oracle AVDF 20.13, you can modify the severity of an assessment. This allows administrators to lower or raise the priority of certain findings depending on how critical they are to their environment. By updating the severity of an assessment, future reports will reflect the modified risk level. This helps prioritize remediation efforts based on the actual perceived risk without ignoring critical security assessments. It also ensures that any changes made will automatically revert after the expiration date unless extended.

To update the severity of an assessment:

1. Click on the **Reports** tab.
2. Click **Assessment** Reports in the left navigation.
3. Choose the assessment you want to update. You can select an assessment across different targets. For instance, to update the severity of "`Database Backup`" for targets tgt1, tgt2, and tgt3, use the multi-select feature.
4. Click on the **Add Exception** button.
5. In the dialog box that appears, choose the new severity from the available options.

> **Note:**
>
> Severity cannot be changed to "Advisory".

6. Optionally, you can enter a justification explaining why the severity is being updated, and provide an expiration date for the update. This expiration date determines how long the customized severity will remain in effect. If expiration date is not mentioned then the severity will be updated until it is reverted manually.
7. Click **Save** to apply the severity update.

8.5.4.2 Deferring an Assessment

In Oracle AVDF 20.13, you can defer an assessment, temporarily excluding it from regular security reports. This is useful when an issue is known but not immediately actionable, or when remediation is planned for a later date. By deferring an assessment, administrators can focus on other priorities without having the issue flagged repeatedly in ongoing reports.

To defer an assessment:

1. Click the **Reports** tab.
2. Click **Assessment Reports** in the left navigation.
3. Click on **Detailed Report** to access more specific assessment details.
4. Select the assessment you wish to defer. As with updating severity, you can choose multiple targets at once. For example, to defer "`Database Backup`" assessment for targets tgt1, tgt2, and tgt3, you can use multi-select feature.
5. Click the **Add Exception** button.
6. In the dialog box, switch the radio button to **Defer Assessment**.
7. Optionally, you can provide justification for the deferral and an expiration date which specify how long the deferral should remain in effect.
8. Click **Save** to defer the assessment.

> **Note:**
>
> Deferred assessments will not appear in any reports (other than the exception report) until the expiration date. However, if you choose not to specify the expiration date, the assessments will be completely deferred.

8.5.5 Revert Exception for Security Assessment Reports

Starting in Oracle AVDF 20.13, you can revert the exception that was added for an assessment

1. Click the **Reports** tab.
2. Click **Assessment Reports** in the left navigation.
3. Click **Exception Report**.
4. Select all the exceptions that need to be reverted.

   > **Note:**
   >
   > The assessments for which severity was updated will be reverted back to the original as defined by Oracle when assessment was done.

5. Click **Revert**.

8.5.6 Severity Levels

The assessment reports include the following severity levels:

- **High Risk**: Needs immediate attention.
- **Medium Risk**: Plan to address this in the short term.
- **Low Risk**: Might be fixed during a scheduled downtime or bundled together with other maintenance activities.
- **Advisory**: Improve security posture by enabling more security features and technology.
- **Evaluate**: Needs manual analysis.
- **Pass**: No risks found.

8.5.7 Categories and Assessments

The Oracle Database Security Assessment (DBSAT) Report begins with a comprehensive summary, followed by detailed findings organized into updated categories for improved clarity and analysis.

The following table lists the categories and descriptions of all assessments that are performed.

Category	Assessment	Description
Auditing	Audit Account Management Activities	Displays whether the actions related to account management are audited by enabled audit policies.

Category	Assessment	Description
Auditing	Audit Administrative (SYS*) Users	Displays whether the actions of the SYS user are audited by enabled audit policies.
Auditing	Audit Database Management Activities	Displays whether the actions related to database management are audited by enabled audit policies.
Auditing	Audit Object Actions	Displays information about the object access audited by enabled audit policies.
Auditing	Audit Powerful Privileges	Displays whether the use of powerful system privileges are audited by enabled audit policies.
Auditing	Audit Privilege Management	Displays whether the actions related to privilege management are audited by enabled audit policies.
Auditing	Audit Records	Displays information about audit trails.
Auditing	Audit Roles with System Privileges	Displays information about the privileges audited by enabled audit policies.
Auditing	Audit SQL Statements	Displays information about SQL statements audited by enabled audit policies.
Auditing	Audit System Privileges	Displays information about the privileges audited by enabled audit policies.
Auditing	Audit User Logon / Logoff	Displays whether database connections are audited by enabled audit policies.
Auditing	Fine Grained Audit	Displays whether fine-grained audit policies are enabled.
Auditing	Unified Audit Policies	Displays whether unified audit policies are enabled.
Auditing*	Audit Synonym Management Activities	Displays information on whether synonym management activities (CREATE ANY SYNONYM, CREATE PUBLIC SYNONYM, CREATE SYNONYM, DROP PUBLIC SYNONYM, DROP SYNONYM) are audited.
Auditing*	Audit Conditions	Lists all audit policies with conditions and, if enabled, lists users/roles it's enabled for.
Auditing*	Audit Shared Accounts	Checks to see if users listed in USER.SHARED are being audited.

Category	Assessment	Description
Auditing*	Audit Storage	Displays information about tablespaces used by different audit trails. Checks include: • Audit trail is SYSTEM • Audit trail is SYSAUX • Tablespace is non-autoextensible & 80% or more full (MEDIUM) • Tablespace is non-autoextensible & 90% or more full (HIGH)
Auditing*	Audit Data Pump	Displays whether data pump exports and imports are being audited.
Auditing*	Audit STIG Actions	Oracle provides out-of-the-box audit policies that aim to answer DoD- auditable events requirements - `ORA_STIG_RECOMMENDATIONS`, `ORA_ALL_TOPLEVEL_ACTIONS and ORA_LOGON_LOGOFF`. This check will validate if these policies are audited.
Auditing*	Audit Oracle Label Security	Displays information regarding enabled audit policies used to audit OLS. • Checks to see if Oracle Label Security (OLS) is enabled and no audit policy is found with OLS action • Reports if OLS is enabled and audit policies were found for OLS actions
Authorization Control	Database Vault	Displays whether Oracle Database Vault is enabled.
Authorization Control	Privilege Analysis	Displays whether privilege analysis is enabled.
Authorization Control*	Authentication for Client Scripts	Lists password-authenticated users whose passwords can potentially be embedded in client scripts, jobs, and application source code to connect to the database server.
Authorization Control*	Data Masking	Lists tables with sensitive data that should be masked when transferred to non-production systems. This check lists tables marked sensitive by TSDP or in `DBA_TABLES` and users that can transfer data via `DATAPUMP_EXP_FULL_DATABASE` or `DATAPUMP_IMP_FULL_DATABASE`.

Category	Assessment	Description
Authorization Control*	PKI Based Authentication	List user accounts identified externally where the authentication method is TCPS. This finding is targeting mostly customers looking for STIG compliance.
Database Configuration	Access to Password File	Displays whether the password file is configured correctly.
Database Configuration	Database Backup	Displays information about database backup records.
Database Configuration	Database Links	Displays information about database links.
Database Configuration	Directory Objects	Displays information about directory objects.
Database Configuration	Disabled Constraints	Displays information about disabled constraints.
Database Configuration	External OS Authorization	Displays whether roles granted to users are controlled by GRANT statements in the database or by the database server's operating system.
Database Configuration	Inference of Table Data	Displays whether data inference attacks are properly blocked.
Database Configuration	Instance Name Check	Displays whether the instance name contains the database version number.
Database Configuration	Network Access Control	Displays information about network access control lists (ACLs).
Database Configuration	Network Communication	Displays information about the initialization parameters for the local network listener.
Database Configuration	Trace Files	Displays information about the initialization parameters for trace files.
Database Configuration	Triggers	Displays information about logon triggers.
Database Configuration	XML Database Access Control	Displays information about XML Database access control lists (ACLs).
Database Configuration*	Authentication Configuration	Displays information about the user account initialization parameters.
Database Configuration*	PDB OS User	Checks if the highly privileged Oracle OS user is set for the PDB_OS_CREDENTIAL parameter.
Database Configuration*	Control Files	Checks if control files are multiplexed and lists all the control file locations.

Category	Assessment	Description
Database Configuration*	Redo Log Files	Checks if the defined redo log files follow best practices and lists their location. Redo logs should be multiplexed and stored on different physical disks.
Database Configuration*	Archive Log Mode	Checks if the database is in `ARCHIVELOG` or `NOARCHIVELOG` mode. If set, also displays the `archive_log_destination` or the `recovery_file_destination`. Also displays the `archive_log_destination` or the `recovery_file_destination` for the standalone databases.
Database Configuration*	Job Details	Checks the scheduled database jobs and users who can administer them. Checks include: • Users who can create database jobs • Jobs that can use privileges of DBA/PDB_DBA
Database Configuration*	Source Code Analysis	Checks `DBA_SOURCE` for non-oracle maintained procedures and functions using `RAISE_APPLICATION_ERROR` and `DBMS_OUTPUT.PUT_LINE`.
Encryption	FIPS Mode for TDE and DBMS_CRYPTO	Displays whether Federal Information Processing Standard (FIPS) 140-2 mode is enabled for Transparent Data Encryption (TDE) and DBMS_CRYPTO.
Encryption	Transparent Data Encryption	Displays whether encryption of tablespace and column data is enabled.
Encryption*	FIPS mode for TLS	Federal Information Processing Standard (140-2) is a U.S. government security standard that specifies security requirements. The SSLFIPS_140 parameter configures the Transport Layer Security (TLS) adapter to run in FIPS mode. SSLFIPS_LIB sets the location of the FIPS library.
Fine-Grained Access Control	Data Redaction	Displays whether data redaction policies are enabled.
Fine-Grained Access Control	Label Security	Displays whether Oracle Label Security is enabled.
Fine-Grained Access Control	Real Application Security	Displays whether Real Application Security (RAS) policies are enabled.

Category	Assessment	Description
Fine-Grained Access Control	Transparent Sensitive Data Protection (TSDP)	Displays whether Transparent Sensitive Data Protection (TSDP) policies are enabled.
Fine-Grained Access Control	Virtual Private Database	Displays whether Virtual Private Database (VPD) policies are enabled.
Privileges and Roles	Access Control Exemption Privileges	Displays access control exemption privileges that are enforced.
Privileges and Roles	Access to Audit Objects	Displays access to audit objects granted to users.
Privileges and Roles	Access to Password Verifier Tables	Displays access to password verifier tables granted to users.
Privileges and Roles	Account Management Privileges	Displays account management privileges granted to users.
Privileges and Roles	All Roles	Displays all roles granted to users.
Privileges and Roles	Audit Management Package	Displays audit management tool access granted to users.
Privileges and Roles	Audit Management Privileges	Displays audit management privileges granted to users.
Privileges and Roles	Broad Data Access Privileges	Displays data access privileges granted to users.
Privileges and Roles	Code Based Access Control	Displays all program units granted code based access control (CBAC) roles.
Privileges and Roles	Column Privileges Granted to PUBLIC	Displays the column access privileges granted to all users.
Privileges and Roles	Data Exfiltration	Displays the user accounts that have been granted rights to access or copy any data from a client or server.
Privileges and Roles	Database Management Privileges	Displays database management privileges granted to users.
Privileges and Roles	Java Permissions	Displays the user accounts that have been granted privileges to execute Java classes within the database.
Privileges and Roles	Role and Privilege Management Privileges	Displays privilege management privileges granted to users.
Privileges and Roles	Roles Granted to PUBLIC	Displays the roles granted to all users.
Privileges and Roles	System Privilege Grants	Displays the system privileges granted to users.
Privileges and Roles	System Privileges Granted to PUBLIC	Displays the system privileges granted to all users.
Privileges and Roles	User Impersonation Privilege	Displays the user accounts that have been granted rights to impersonate other users.
Privileges and Roles	Users with Administrative SYS* Privileges	Displays the administrative privileges granted to user accounts.

Category	Assessment	Description
Privileges and Roles	Users with DBA Role	Displays the user accounts that have been granted the DBA role.
Privileges and Roles	Users with Powerful Roles	Displays the user accounts that have been granted roles with maximum data access privileges.
Privileges and Roles	Write Access to Restricted Objects	Displays access to restricted objects granted to users.
Privileges and Roles*	Encryption Packages Granted to PUBLIC	Displays DBMS_CRYPTO, DBMS_OBFUSCATION_TOOLKIT, and DBMS_RANDOM grants to PUBLIC
Privileges and Roles*	Scheduler Job Packages Granted to PUBLIC	Display DBMS_SCHEDULER and DBMS_JOB EXECUTE grants to PUBLIC and Scheduler/Job system privileges (CREATE JOB, MANAGE SCHEDULER, CREATE EXTERNAL JOB, CREATE ANY JOB) grants to PUBLIC.
Privileges and Roles*	Credential Package Granted to PUBLIC	Displays EXECUTE grant on DBMS_CREDENTIAL package to PUBLIC. Also checks for privilege grants of CREATE CREDENTIAL and CREATE ANY CREDENTIAL to users.
Privileges and Roles*	File System Packages Granted to PUBLIC	Displays EXECUTE grant on DBMS_LOB, UTL_FILE, and DBMS_ADVISOR packages to PUBLIC. Also checks for system privilege grants of CREATE ANY DIRECTORY and DROP ANY DIRECTORY to users.
Privileges and Roles*	Network Packages Granted to PUBLIC	Displays EXECUTE grant on DBMS_LDAP, UTL_HTTP, UTL_INADDR, UTL_SMTP, and UTL_TCP packages to PUBLIC. Also checks for users that are authorized to execute packages via ACLs.
Privileges and Roles*	SQL Packages Granted to PUBLIC	Displays EXECUTE grant on DBMS_XMLQUERY, DBMS_XMLSAVE, DBMS_XMLSTORE, DBMS_REDACT, DBMS_XMLGEN, and DBMS_SQL packages to PUBLIC.
Privileges and Roles*	JAVA Permissions Granted to PUBLIC	Displays EXECUTE grant on DBMS_JAVA and DBMS_JAVA_TEST packages to PUBLIC. Also checks for grants of JAVA_ADMIN role to users
Privileges and Roles*	Users Who Can Impersonate Other Users	Displays the user accounts that have been granted rights to impersonate other users.

Category	Assessment	Description
Privileges and Roles*	Privilege for Data Exfiltration in Bulk	Displays the user accounts that have been granted rights to access or copy any data from a client or server.
User Accounts	Account Locking after Failed Login Attempts	Displays information about user profile failed login attempt enforcement.
User Accounts	Case-Sensitive Passwords	Displays whether case-sensitive passwords are enabled.
User Accounts	Inactive Users	Displays information about the user accounts that are not in use and also accounts that are not configured to be locked when inactive.
User Accounts	Password Verification Functions	Displays information about password verification functions enforcement.
User Accounts	Password Verifiers	Displays information about the user accounts with obsolete password verifiers.
User Accounts	Sample Schemas	Displays information about the user accounts that use sample schemas such as SCOTT, HR, OE, SH, PM, IX, ADAMS, BLAKE, CLARK, and BI.
User Accounts	User Parameters	Displays information about the user account initialization parameters.
User Accounts	User Schemas in SYSTEM or SYSAUX Tablespace	Displays information about the regular user accounts that use the reserved Oracle-supplied tablespaces.
User Accounts	Users with Default Passwords	Displays information about the user accounts with default passwords.
User Accounts	Users with Expired Passwords	Displays information about the user accounts with expired passwords.
User Accounts	Users with Unlimited Concurrent Sessions	Displays all users that have a profile resource limit for SESSIONS_PER_USER set to UNLIMITED. With SESSIONS_PER_USER = UNLIMITED users can have any number of concurrent sessions.
User Accounts	Users with Unlimited Password Lifetime	Displays information about user profile password expiration enforcement.
User Accounts*	Users with DEFAULT Profile	Displays the DEFAULT user profile password and resource parameters and the number of users in it.

Category	Assessment	Description
User Accounts*	Application Owner Account	Checks the database for the account that could be considered the application owner and for objects accessible by the application owner.
User Accounts*	Shared Accounts	Displays users that have multiple administrative privileges and proxy users.
User Accounts*	Users with Objects	Displays application users who own objects and can grant access to those objects to other users
User Accounts*	Users Authorized for Object Ownership	Displays non-oracle maintained users who own objects
User Accounts*	Users with Security Objects	Displays users who own security objects
User Accounts*	Users with Grant Option	Checks for users that have been granted privileges with `WITH GRANT OPTION`.
User Accounts*	Users with Sensitive Data	Displays users that own tables with columns marked as sensitive with TSDP and users that can access those tables.
User Accounts*	Legacy Password Versions	Displays information about the user accounts with obsolete password verifiers.
User Accounts*	Users with no Password Complexity Requirements	Displays information about profiles with and without a password complexity verification function. Users not subject to password complexity verification are also displayed.
User Accounts*	Unlimited Session Idle Time	This check lists users with `UNLIMITED IDLE TIME`.
User Accounts*	Users with Gradual Password Rollover	Displays information about the Gradual Password Rollover.
User Accounts*	Temporary Users	Displays users associated with the DEFAULT profile.
User Accounts*	Development Users in Production Databases	There should not be developer accounts in production systems. Verify if such accounts exist in your database.
Basic Information*	Patch Check	Displays information about the patches installed.

Note:

* Signifies assessments that have been added in Oracle AVDF 20.13.

8.6 AVDF System Reports

Starting in Oracle AVDF 20.13, the results of AVDF application auditing can be viewed by a `super auditor` on the **AVDF System Report** page.

1. Log in to the Audit Vault Server Console as a `super auditor`.
2. Click on the **Reports** tab.
3. Click on **AVDF System Reports**.
   You will see the following reports:
   - **All Activity** - The All Activity report includes all the audited activities of the AVDF appliance's application, embedded repository, and operating system.
   - **Application Auditing** - The Application Auditing report includes all the audited activities of the AVDF appliance's application.
   - **Database Auditing** - The Database Auditing report includes all the audited activities of the AVDF appliance's embedded repository.
   - **OS Auditing** - The OS Auditing report includes all the audited activities of the AVDF appliance's embedded operating system.

Related Topics

- Monitoring in AVDF 20.13 and later

8.7 Customizing Reports

You can customize existing reports by using built-in tools to filter, group, and highlight data and define columns. These customized reports can be saved as new report formats and accessed from the **Saved Reports** tab. Saved custom formats of existing reports can only be viewed online as they can't be scheduled or printed in PDF format.

8.7.1 Filtering Data in a Report

You can filter the report to show data based on a search, a particular value, or an expression. Starting in Oracle AVDF 20.11, you can also filter the All Activity Report based on a Global Set, as well as filter Compliance GDPR Reports (including Sensitive Data, Access Rights to Sensitive Data, Activity on Sensitive Data, and Activity on Sensitive Data by Privileged Users) based on a Sensitive Objects Set.

You can control the display of data in a report to focus on a particular set of data. Oracle Audit Vault and Database Firewall 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 Also:

Saving your Customized Reports

8.7.1.1 Filtering by Search

Learn about filtering rows and columns 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*.
2. Click the **Reports** tab, and then access the report that you want.
3. 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.
4. In the Search bar text area, enter all or part of the row text you want to search for.
5. Click **Go**.

> **See Also:**
>
> Logging in to the Audit Vault Server Console

8.7.1.2 Filtering by a Data Value

Learn about filtering all the rows based on selected data in a 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*.
2. Click the **Reports** tab, and then access the report that you want.
3. 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.
4. For **Filter Type**, select **Column**.
5. 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.
6. Select the **Operator** and **Expression** that you want to use, to further filter the data.
7. Click **Apply**.

   The existing filter definitions for the current user session are shown above the report columns.
8. To enable or disable the display of the filtered data, select its corresponding check box. To remove a filter, click its **Remove Filter** icon.

See Also:

Logging in to the Audit Vault Server Console

8.7.1.3 Filtering by an Expression

Learn about filtering data in rows 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*.
2. Click the **Reports** tab, and then access the report that you want.
3. 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.
4. For **Filter Type**, select **Row**.
5. Enter a **Name** for the filter.
6. 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.

     For example: To view login failure events in the report, use the following filter condition:

     ```
     event_name IN (‘LOGIN’,’LOGON’) and event_Status = ‘FAILURE’
     ```

     As you build the expression, the **Filter Expression** field is populated with the expression.
7. Click **Apply**.

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

See Also:

Logging in to the Audit Vault Server Console

8.7.1.4 Filtering by a Global Set in an All Activity Report

Learn about applying a Global Set filter on an All Activity Report.

Starting in Oracle AVDF 20.11, this method filters relevant data to a selected Global Set in an All Activity Report. The user may choose one or more of the following Global Set types:

- IP Address Set
- OS User Set
- Client Program Set
- Database User Set
- Privileged User Set
- Sensitive Object Set

To apply a Global Set filter on an All Activity Report:

- AVDF 20.13 and later
- AVDF 20.10 and later

AVDF 20.13 and later

1. Log in to the Audit Vault Server Console as an `auditor`.
2. Click the **Reports** tab.
3. Select the **All Activity** report.
4. Click on **Actions**.
5. Click **Filter**.
6. Select a column that corresponds for use with a global set:

Column	Global Set
Client IP	IP Address Set
OS User	OS User Set
Client Program	Client Program Set
User	Database User Set Privileged User Set
Object	Sensitive Object Set

7. Select an operator: only `=`, `!=`, `in`, and `not in` are supported operators for Global Sets.
8. Enter the global set name as the **Expression**.
9. Click **Apply**.

AVDF 20.10 and later

1. Log in to the Audit Vault Server Console as an `auditor`.
2. Click the **Reports** tab.
3. Select the **All Activity** report.
4. Click on **Actions**.
5. Click **Select Columns**.
6. Choose one or more of the Global Set based columns.
7. Click **Apply**.
8. Click on an added Global Set column heading to show filter values.
9. Select one of the Global Set names to apply the filter.

Related Topics

- Global Sets - Oracle AVDF 20.10 and later
  Starting in Oracle AVDF 20.10, Global Sets allows you to create global IP Address, OS User, Client Program, and Database User sets on any type of target database. In addition you can create global Privileged User and Sensitive Objects sets on Oracle Database targets.

8.7.1.5 Filtering on Sensitive Objects in Compliance GDPR Reports

Learn about filtering the content of a Compliance GDPR Report (including Sensitive Data, Access Rights to Sensitive Data, Activity on Sensitive Data, and Activity on Sensitive Data by Privileged Users) using a filter based on Sensitive Objects Set.

Starting in Oracle AVDF 20.11, users can filter the content of a Compliance GDPR Report using a filter based on Sensitive Objects Set.
To apply a Sensitive Objects Set filter on a Compliance GDPR Report:

1. Log in to the Audit Vault Server as an *auditor*.
2. Click the **Reports** tab.
3. Click on the **Compliance Reports** tab.
4. Select **Sensitive Objects** report
5. Click on **Actions**, then click **Select Columns**.
6. Click on Sensitive Objects Set column header.
7. Choose the Sensitive Objects Set to apply the filter.
8. Click **Apply**.

> **See Also:**
>
> - Logging in to the Audit Vault Server Console
> - Configuring Compliance Reports

8.7.2 Formatting Data in a Report

Learn how to format data viewed in a report.

8.7.2.1 Sorting Row Data for All Columns

Learn to sort data in rows for all the columns.

To sort row data for all columns:

1. Log in to the Audit Vault Server as an *auditor*.
2. Click the **Reports** tab, and then access the report that you want.
3. From the **Actions** menu, select **Format**, then select **Sort**.

   The **Sort** dialog box appears.
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**.

> **See Also:**
>
> Logging in to the Audit Vault Server Console

8.7.2.2 Highlighting Rows in a Report

Learn how to highlight 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. Log in to the Audit Vault Server as an *auditor*.
2. Click the **Reports** tab, and then access the report that you want.
3. From the **Actions** menu, select **Format**, then **Highlight**.

   The **Highlight** dialog box appears.
4. Enter the following information:
   - **Name:** Optionally enter a name for this highlight instance.
   - **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. Click outside of the color selection dialog once done.
- **Text Color:** Select a text color for the row or cell using the same method you used for the background color. Click outside of the color selection dialog once done.
- **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**.

> **See Also:**
>
> Logging in to the Audit Vault Server Console

8.7.2.3 Creating a Chart from Report Data

Learn how to chart 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. Log in to the Audit Vault Server as an *auditor*.
2. Click the **Reports** tab, and then access the report that you want.
3. From the **Actions** menu, select **Format**, then **Chart**.

   The **Chart** dialog box appears.
4. Enter the following information:
   - **Chart Type:** Select from one of the four chart styles: **Bar**, **Line with Area**, **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.
- **Orientation:** Choose Landscape or Portrait.

5. Click **Apply**: Select vertical or horizontal.

   The chart appears, with the **Edit Chart** and **View Report** links under the search bar.

> **See Also:**
>
> Logging in to the Audit Vault Server Console

8.7.2.4 Adding Control Breaks to a Report

Learn to add control breaks to selected columns in a report.

You can create a break group based on selected columns. This pulls the column out of the report as a main record and groups all rows with the same value for the selected column under that main 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 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 Target Name.

To add a control break in a column:

1. Log in to the Audit Vault Server as an *auditor*.
2. Click on **Reports** tab, and then access the report that you want.
3. From the **Actions** menu, select **Format**, then **Control Break**.
4. Select the columns 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. Selecting **Enabled** adds a control break; selecting **Disabled** removes the control break.
5. Click **Apply**.

> **See Also:**
>
> Logging in to the Audit Vault Server Console

8.7.2.5 Using the Group By Feature to Format a Report

Learn to format a report using the Group By option.

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 target and client IP address combination. Using Group By, you can create a custom report to group unique targets together in the first column, client IP addresses for each 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 target and client IP address combination.

The resulting custom report will contain four columns: 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 target and IP address.

To use the Group By feature:

1. Log in to the Audit Vault Server as an *auditor*.
2. Click the **Reports** tab, and then access the report that you want.
3. From the **Actions** menu, select **Format**, then **Group By**.

   The **Group By** dialog is displayed.
4. In the **Group By Column** field, 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 Target Name, column 1 of your report will have targets grouped together. Optionally, select data groupings for columns 2 and 3 of your report.
5. Optionally, in the **Functions** field, specify up to three functions to operate on specific data columns. For example, Count Distinct.
6. Under **Column**, select any data column in the default report.
7. Optionally, under **Label** enter a column heading for the new column created by the result of this function.
8. Optionally, under **Format Mask** select the format of the data in the new column created by the result of this function.
9. Optionally, select the **Sum** check box if you want to add a **Sum** row to the bottom of your custom report to add the values in the new column.
10. Click **Apply**.

> **See Also:**
>
> Logging in to the Audit Vault Server Console

8.7.3 Hiding or Showing Columns in a Report

Learn to hide or show columns in reports.

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*.
2. Click the **Reports** tab, and then access the report that you want.
3. From the **Actions** menu, click **Select Columns**.

   The **Select Columns** dialog field appears.
4. 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.

5. 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.
6. Click **Apply**.

> **See Also:**
>
> Logging in to the Audit Vault Server Console

8.7.4 Customized Reports

8.7.4.1 Saving your Customized Reports

Learn how to save customized reports.

When you customize a built-in report with your specified filters and display settings, you can save this customized report. Such reports are listed in the **Saved Reports** tab 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*.
2. Click the **Reports** tab, and then access the report that you want.
3. Filter and design the display as needed.
4. From the **Actions** menu, select **Save Report**.
5. Enter the following information in the **Save Report** dialog box:
   - **Name:** Enter a name for the report.
   - **Description:** Enter a brief description of the report.
   - **Public:** Select this check box to make the report accessible to all users.
6. Click **Apply**.

   The custom report is listed on the **Saved Reports** tab.

> **See Also:**
>
> - Filtering Data in a Report
> - Logging in to the Audit Vault Server Console

8.7.4.2 Accessing Your Saved Custom Reports

Learn how to access 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.
3. Click **Saved Reports** tab in the left navigation menu.

   The **Saved Reports** page appears.
4. In the **Name** column, select the link for the specific report.

   The report page is displayed. From here, you can:

   - Click the saved report name above the filter to edit it.
   - Click a filter to modify it. Alternately, you can click on **Actions** menu, and then click on **Filter**.
   - Remove a filter by clicking the Remove Filter icon (an "X")
   - Enable or disable a control break by selecting or deselecting its check box
   - Remove a control break by clicking the Remove Breaks icon (an "x")

> **Note:**
>
> Saved reports can't be scheduled.

Related Topics

- Filtering Data in a Report
  You can filter the report to show data based on a search, a particular value, or an expression. Starting in Oracle AVDF 20.11, you can also filter the All Activity Report based on a Global Set, as well as filter Compliance GDPR Reports (including Sensitive Data, Access Rights to Sensitive Data, Activity on Sensitive Data, and Activity on Sensitive Data by Privileged Users) based on a Sensitive Objects Set.
- Logging in to the Audit Vault Server Console
  To log in to the Audit Vault Server console, you must have a valid user name and password.

8.7.5 Creating and Scheduling a Custom Report

Learn how to create and schedule a custom report.

While a customized view of an existing report can be accessed from the **Saved Reports** tab, a custom report can be created and scheduled from the **PDF/XLS Reports** tab (**Report**

Templates tab starting in Oracle AVDF release 20.8). Scheduling a custom report is not available by default. Follow these steps to schedule a custom report:

1. Log in to the Audit Vault Server as an *auditor*.
2. Click the **Reports** tab.
3. Click **PDF/XLS Reports** tab (**Report Templates** tab starting in Oracle AVDF release 20.8) in the left navigation menu.
4. In the **Built-in Reports** section, click the icons under **Download Report Template** and **Download Report Definition** columns.
5. Save the files to your local machine.
6. Modify the template and definition similar to any custom report.
7. Click **Upload** button.
8. Choose the template file and definition file in the dialog.
9. Optionally enter the **Description**.
10. Click **Save**.
11. The newly uploaded report template and definition is visible in the **PDF/XLS Reports** section (**Report Templates** section starting in Oracle AVDF release 20.8).
12. Click the icon under **Schedule Report** column.
13. Configure the report schedule details.
14. After the report is generated, it is accessible in the **Generated Reports** tab.
15. The report can be downloaded.

8.7.6 Resetting the Report Display Values to Their Default Settings

Learn how to reset display of values in reports.

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

To reset the display settings to their defaults:

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

   The **Reset** dialog appears with the following message:

   ```
   Restore report to the default settings.
   ```
4. Click **Apply**.

> **See Also:**
>
> Logging in to the Audit Vault Server Console

8.8 Creating Non-Interactive Report Templates

You can create, modify, and use existing PDF or XLS report templates.

Prerequisites

- BI Publisher Desktop is installed on Microsoft Windows host.

  BI Publisher can be downloaded from Oracle Technical Resources.
- User is able to log in to Audit Vault Server through console.
- Information pertaining to the *AVSYS* schema holding audit data is available.

8.8.1 Creating Non-Interactive Report Template

You can create a new non-interactive or PDF/ XLS report, using an existing RTF or an XML report.

1. Log in to the Audit Vault Server console as *auditor*.
2. Click **Reports** tab and then click on **PDF/XLS Reports** tab (**Report Templates** tab starting with Oracle AVDF release 20.8) in the left navigation menu.

   Result:
   The page displays all the configured reports in two sections **PDF/XLS Reports** (**Report Templates** starting with Oracle AVDF release 20.8) and **Built-in Reports**.
3. Click on the icon against any of the existing reports under the **Download Report Template** column.
4. Save the report to your local drive with a new name.
5. To preview changes in the RTF file requires sample data. Write a new Report SQL Query referring to the existing SQL in sample report XML file.
6. The above SQL Query output is generated from SQL Developer and is exported into XML format. It is not compatible with RTF files. To generate data in RTF required XML format, use the `DBMS_XMLGEN.GETXML ()` function. This is a built in function of Oracle Database.
7. To generate XML data, use the SQL query string as a parameter to `dbms_xmlgen.getxml()` function.

   Result:
   It returns XML data as output.

   The below SQL example is for reference only.

   ```
   SELECT DBMS_XMLGEN.GETXML (‘YOUR REPORT SQL QUERY WITH PARAMETERS’) xml_data
   FROM dual;
   ```

   Example:

   ```
   SELECT DBMS_XMLGEN.GETXML('SELECT TO_CHAR(event_time, ''DS TS'') AS
   event_time,
   event_name,
   target_object,
   event_status,
   user_name,
   client_ip,
   client_program,
   ```

```
secured_target_name,
COUNT(*) OVER () AS totalrowcount,
COUNT(secured_target_name) OVER(PARTITION BY secured_target_name) AS
securerowcount
FROM avsys.event_log elog
WHERE ROWNUM <= 3000
AND ( event_time BETWEEN ''19-DEC-13 09.35.02.570000000 AM'' AND ''20-
DEC-13 09.35.02.570000000 AM'' )
AND secured_target_id IN(SELECT secured_target_id FROM
avsys.secured_target
                        WHERE (

(secured_target_name_vc=UPPER(''MSSQLKVM5'')
                                  OR
                                  secured_target_name_vc LIKE
UPPER(''MSSQLKVM5''||''_DELETED%'')
                                )
                                  OR
                                  UPPER(''MSSQLKVM5'')=''ALL''
                              )
                            )
ORDER BY secured_target_name, elog.event_time') xml
from dual;
```

> **Note:**
>
> To generate SQL query string, use additional single quote inside this function for character identifier as escape character.
>
> For example:
>
> a. For `DS TS` date and timestamp formatting, apply single quote (') as escape character.
>
> b. For *event_time* timestamp parameter provide value as `''19-DEC-13 09.35.02.570000000 AM''`.
>
> > **Note:**
> >
> > Insert two single quotation marks for defining parameters.
>
> c. For *database_name* parameter provide value as `''MSSQL_ST''`.
>
> d. Numeric values can be provided as is. Provide value for *ROW_LIMIT* parameter as `3000` or `20000` (any numerical value). Similarly make changes to other strings and parameters in the SQL query using single quotes.

8. Copy the query output from SQL Developer tool (or any other tool).

9. Paste it into notepad and save this file as XML.

10. There is another option to use SPOOL command to generate XML file. See Generating XML Data File Using SPOOL Command for complete information. Load the generated XML file.

11. Open the RTF template or sample report downloaded earlier using Microsoft Word.
12. Click on **BI Publisher** tab on the top right corner.
13. Click on **Load XML** and navigate to the generated XML and load it.

    Result:
    The following message is displayed:

    ```
    Data loaded successfully.
    ```

14. Make the necessary changes to the report.
15. If the file is in *RTF* format, then continue with the next step. Else, skip the remaining steps as they are relevant only for *RTF* files. Use Microsoft Word to edit the *RTF* file.
16. Change the existing report name.
17. Change report parameters like `REPORT PERIOD`, `RUN BY`, and `REPORT RECORD LIMIT` if required.
18. Change the report parameter label if required.

    For example:

    Change the label `RUN BY`, you can change it directly to `RUN BY USER`.

19. Change the report parameter value if required. This is the SQL query column name.

    For example:

    To change the `TIME_FROM` value double click on *TIME_FROM*. Or right click on it to access **BI Publisher**, then select **Properties**, and **Advanced** tab. To change `<?TIME_FROM?>` to data XML column name and the XML tag name for this column is `TIME1`, so your tag will be `<?TIME1?>`.

20. To change existing chart double click on it and change `VALUES`, `AGGREEGATION`, `LABELS`, `TYPE`, and `STYLE` parameters. In case the chart is not required, then delete it.
21. Change data table labels in the report if required. If the data table columns are different, the change the label and values as mentioned in earlier steps. To add additional columns, right click on the table, select **Insert**, and then select **Insert columns to the Right.** Similarly the columns can be merged and deleted.
22. Change report header name if required.
23. Choose to display target level count and level count.
24. Retain the Time Zone and Date in footer section as they are common to all the reports.
25. Click on the **PDF** or **Excel** icon in the tab to verify the changes.
26. In case all the changes meet the requirements, then save the RTF file.

    > **Note:**
    >
    > In the generated PDF report, data for parameters is not be displayed in header section. The parameters data is sourced from application runtime.

27. This RTF report file can be uploaded along with XML report file for verification.
28. Create the XML file.

    The following are the different tags in XML report file:

a. **Parameter:** Add or change input report parameters in this tag if new report parameters are different.

b. **DATA**: Contains the following tags or headers:

   - `Column 1`: Data Tag
   - `Column 2`: Description
   - `AUDIT_SUBREPORT`: Displays parameter values on RTF files in the header section. These change as per the new report parameters.
   - `Time zone`: Displays time zone information and is common for all the reports. This need not be changed.
   - `TLQR`: Contains report SQL and column mappings which should map with RTF column values. In this section, you need to paste your new report SQL query and column alias name mapping in XML column and values tags.

29. This XML report file can be uploaded along with the RTF file generated earlier.

> **Note:**
>
> RTF and XML file names must be same.

30. Navigate to the uploaded reports section in Audit Vault Server console and click **Upload**.
31. Provide updated RTF and unchanged report definition taken from earlier steps.
32. Verify the report in the **Generated Report** section under the **Reports** tab of the Audit Vault application.
33. In case the report is not generated, then check the status of the report in **Settings** tab, and then select **Jobs** in the left navigation menu.

8.8.2 Modifying Non-Interactive Report Template

You can modify or make cosmetic changes to Audit Vault reports.

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

   Result:
   The page displays the following reports in multiple sections:

   - **Activity Reports**
     - **Summary**
     - **Data Access & Modification**
     - **Login & Logout Events**
     - **Database Settings**
   - **Entitlement Reports**
   - **OS Correlation Reports**
   - **Database Firewall Reports**
   - **Stored Procedure Changes**

- **DB Vault Activity**

3. Click **PDF/XLS** sub tab in the left navigation menu.
4. Click the download icon under `Download Report Template` and `Download Report Definition` file for the specific report.
5. Previewing changes in the RTF file format, requires sample data. Copy the query data from the XML file which is similar to the following. Select the text mentioned below:

   ```
   to_char(event_time, 'DS TS') as event_time
       client_ip,
       user_name,
       osuser_name,
       client_program,
       secured_target_name,
       error_code,
       error_message,
       decode
       {
           audit_trail_id,
           null, 'Network',
           'Audit Trail'
       }    as event_source
   from
       avsys.event.log
   ```

6. The query output generated from SQL Developer and exported into XML format is not compatible with RTF files.
7. To generate XML data, use the `dbms_xmlgen.getxml()` function. This is a built in function of Oracle Database.
8. Pass SQL query string as a parameter to `dbms_xmlgen.getxml()` function.

   Result:
   It returns XML data with sample output mentioned below.

   ```
   SELECT DBMS_XMLGEN.GETXML('SELECT TO_CHAR(event_time, ''DS TS'') AS
   event_time,
   event_name,
   target_object,
   event_status,
   user_name,
   client_ip,
   client_program,
   secured_target_name,
   COUNT(*) OVER () AS totalrowcount,
   COUNT(secured_target_name) OVER(PARTITION BY secured_target_name) AS
   securerowcount
   FROM avsys.event_log elog
   WHERE ROWNUM <= 3000
   AND ( event_time BETWEEN ''19-DEC-13 09.35.02.570000000 AM'' AND ''20-
   DEC-13 09.35.02.570000000 AM'' )
   AND secured_target_id IN(SELECT secured_target_id FROM
   avsys.secured_target
                           WHERE (
   ```

```
(secured_target_name_vc=UPPER(''MSSQLKVM5'')
                                  OR
                                  secured_target_name_vc LIKE
UPPER(''MSSQLKVM5''||''_DELETED%'')
                                )
                                  OR

                                  UPPER(''MSSQLKVM5'')=''ALL''
                              )
                            )
ORDER BY secured_target_name, elog.event_time') xml
from dual;
```

> **Note:**
>
> To generate SQL query string, use additional single quote inside this function for character identifier as escape character.
>
> For example:
>
> a. For `''DS TS''` date and timestamp formatting, apply single quote (') as escape character.
>
> b. For *event_time* timestamp parameter provide value as `''19-DEC-13 09.35.02.570000000 AM''`.
>
> > **Note:**
> >
> > Insert two single quotation marks for defining parameters.
>
> c. For *database_name* parameter provide value as `''MSSQL_ST''`.

9. The above SQL query generates data in XML format, which can be uploaded in BI publisher template (RTF).
10. Copy the query output from SQL Developer tool (or any other tool).
11. Paste it into notepad and save this file as XML.

> **Note:**
>
> There is another option to use SPOOL command to generate XML file. See Generating XML Data File Using SPOOL Command for complete information. Load the generated XML file.

8.8.3 Generating XML Data File Using SPOOL Command

You generate XML from SQL*Plus using the SPOOL command.

1. Take the SQL query used to generate data in XML format.

For example:

```
SELECT DBMS_XMLGEN.GETXML('SELECT TO_CHAR(event_time, ''DS TS'') AS
event_time,
event_name,
target_object,
event_status,
user_name,
client_ip,
client_program,
secured_target_name,
COUNT(*) OVER () AS totalrowcount,
COUNT(secured_target_name) OVER(PARTITION BY secured_target_name) AS
securerowcount
FROM avsys.event_log elog
WHERE ROWNUM <= 3000
AND ( event_time BETWEEN ''19-DEC-13 09.35.02.570000000 AM'' AND ''20-
DEC-13 09.35.02.570000000 AM'' )
AND secured_target_id IN(SELECT secured_target_id FROM avsys.secured_target
                        WHERE (

(secured_target_name_vc=UPPER(''MSSQLKVM5'')
                                  OR
                                  secured_target_name_vc LIKE
UPPER(''MSSQLKVM5''||''_DELETED%'')
                                ) OR
                                  UPPER(''MSSQLKVM5'')=''ALL''
                              )
                            )
ORDER BY secured_target_name, elog.event_time') xml
from dual;
```

2. Unlock the `avsys` user on the Audit Vault Server Database:

   ```
   ssh support@<AuditVaultServer_IP>
   su root
   su dvaccountmgr
   sqlplus /
   alter user avsys identified by <password> account unlock;
   exit;
   ```

3. Connect to the `avsys` user on the Audit Vault Server Database:

   ```
   ssh support@<AuditVaultServer_IP>
   su root
   su oracle
   sqlplus avsys
   <password>
   ```

4. Run the command:

   ```
   spool <path of the xml file>/<name of the xml file>.xml
   ```

5. Run the SQL query from the earlier step.
6. Run the following command to turn off generating the XML data file further:

```
spool off
```

7. Check the XML file generated in the location defined earlier. Remove unwanted strings and retain only the data.
8. Save it.
9. Open the RTF template downloaded earlier.
10. Click on **BI Publisher** tab on the top right corner.
11. Click on **Load XML.**
12. Navigate to the location of the generated XML file.
13. Load it.

    Result:
    The following message is displayed:

    ```
    Data loaded successfully.
    ```

14. Make the necessary changes.
15. To verify the change, click on the **PDF** or **Excel** icon in the tab.
16. If all the changes are complete as expected, save the RTF file.

    > **Note:**
    >
    > In the generated PDF report, data for parameters is not displayed in the Header. These parameters and data is captured during application runtime.

17. Navigate to the uploaded reports section in Audit Vault Server console and click **Upload.**

    > **Note:**
    >
    > RTF and XML file names must be same.

18. Provide updated RTF and unchanged report definition taken from earlier steps.
19. Verify the report on the server.

8.8.4 Generating Reports Using RTF And XML Sample Templates

You can generate reports using RTF and XML sample templates.

1. Use the existing XML and RTF report files.
2. Save them with a new report name.
3. To preview changes to the RTF file, sample data is required. Write a new Report SQL Query.
4. The above SQL Query output is generated from SQL Developer and is exported into XML format. It is not compatible with RTF files. To generate data in required RTF XML format, use the `DBMS_XMLGEN.GETXML ()` function. This is a built in function of Oracle Database.
5. Provide SQL query string as a parameter to `dbms_xmlgen.getxml()` function. Execute:

    ```
    SELECT DBMS_XMLGEN.GETXML ('YOUR REPORT SQL QUERY WITH PARAMETERS') xml_data
    ```

```
FROM dual;
```

Result:
It returns the following example XML data as output:

```
SELECT DBMS_XMLGEN.GETXML('SELECT TO_CHAR(event_time, ''DS TS'') AS
event_time,
event_name,
target_object,
event_status,
user_name,
client_ip,
client_program,
secured_target_name,
COUNT(*) OVER () AS totalrowcount,
COUNT(secured_target_name) OVER(PARTITION BY secured_target_name) AS
securerowcount
FROM avsys.event_log elog
WHERE ROWNUM <= 3000
AND ( event_time BETWEEN ''19-DEC-13 09.35.02.570000000 AM'' AND ''20-
DEC-13 09.35.02.570000000 AM'' )
AND secured_target_id IN(SELECT secured_target_id FROM
avsys.secured_target
                        WHERE (

(secured_target_name_vc=UPPER(''MSSQLKVM5'')
                                  OR
                                  secured_target_name_vc LIKE
UPPER(''MSSQLKVM5''||''_DELETED%'')
                                )
                                  OR
                                  UPPER(''MSSQLKVM5'')=''ALL''

                              )
                            )
ORDER BY secured_target_name, elog.event_time') xml
from dual;
```

> **Note:**
>
> To generate SQL query string, use additional single quote inside this function for character identifier as escape character.
>
> For example:
>
> a. For `''DS TS''` date and timestamp formatting, apply single quote (') as escape character.
>
> b. For *event_time* timestamp parameter provide value as `''19-DEC-13 09.35.02.570000000 AM''`.
>
> > **Note:**
> >
> > Insert two single quotation marks for defining parameters.
>
> c. For *database_name* parameter provide value as `''MSSQL_ST''`.
>
> d. Numeric values can be provided as is. Provide value for *ROW_LIMIT* parameter as `3000` or `20000` (any numerical value).
>
> e. Apply additional single quote (') for string and date parameters, if they are present in SQL query.

6. Copy the query output from SQL Developer tool (or any other tool).
7. Paste it into notepad and save this file as XML.
8. There is another option to use SPOOL command to generate XML file. See Generating XML Data File Using SPOOL Command for complete information. Load the XML data file.

   Result:
   The following message is displayed:

   ```
   Data loaded successfully.
   ```
9. Make the changes to the RTF file as required. Change the report header name.
10. Change the report parameters like `Label` and `Values` if required.

    For example:

    To change the label use option like `RUN BY`.
11. To change the TIME value double click on one of the TIME fields. Or right click on it to access **BI Publisher**, then select **Properties**, and then **Advanced** tab. In the **Advanced** tab, add column reference value in `<?ColumnName?>` format. This column name is a reference of SQL Query output column name.
12. To change the Report Chart go to **BI Publisher** tab, and click on **CHART**. Add chart as per your requirement by providing uploaded XML data as parameters.
13. In the Report Data Table, go to **BI Publisher** tab, and click on **TABLE WIZARD**. Select the columns to be displayed in the table.
14. Change the report header of the second page.
15. In the target group level and total, choose aggregation at target level and total count at report level. Execute:

    ```
    count(*) over () as totalrowcount,
    ```

```
count(secured_target_name) over(partition by secured_target_name) as
securerowcount
```

16. Keep same columns alias so that they can be referred in the report.
17. Retain the Time Zone and Date in footer section as they are common to all the reports.
18. Click on the **PDF** or **Excel** icon in the tab to verify the changes.
19. In case all the changes meet the requirements, then save the RTF file.

> **Note:**
>
> In the generated PDF report, data for parameters is not be displayed in header section. The parameters data is sourced from application runtime.

20. This RTF report file can be uploaded along with XML report file for verification.
21. Create report XML using an existing template. Follow and use the comments existing in the template and modify accordingly. This is the report XML which is used to upload along with RTF file generated earlier.
22. Log in to the Audit Vault Server console as *auditor*.
23. Click **Reports** tab.
24. Click **PDF/XLS Reports** tab (**Report Templates** tab starting with Oracle AVDF release 20.8) in the left navigation menu.
25. Click **Upload** button in the top right corner.

    The **Upload Custom Report** dialog is displayed. Click the fields to choose the file saved in your local machine.

> **Note:**
>
> The RTF and XML file names must be same.

26. Optionally enter the **Description** and click **Save**.
27. Verify the report in the **Generated Reports** tab.
28. In case the report is not generated, then check the status in the **Settings** tab, and then select the **Jobs** tab in the left navigation menu.

8.9 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 Audit Vault and Database Firewall. This section describes how to download these files from an existing Oracle Audit Vault and Database Firewall 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.

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

3. Click **PDF/XLS Reports** tab (**Report Templates** tab starting with Oracle AVDF release 20.8) in the left navigation menu.

   The **PDF/XLS Reports** (or **Report Templates**) page is displayed. It lists previously uploaded custom reports. The built-in reports are listed under the **Built-in Reports** section.
4. Find a built-in report to use as a starting point for your new custom report.
5. Click the **Download Report Template** icon and save the RTF file.
6. Click the **Download Report Definition** icon and save the XML file.
7. Customize the report definition and template files using either **Oracle BI Publisher** or another tool, as necessary.
8. Click **Upload** button located in the top right corner.

   The **Upload Custom Report** dialog is displayed.
9. In the **Report Template file** field, enter the name or browse for your customized report template (RTF) file.
10. In the **Report Definition file** field, enter the name or browse for your customized report definition (XML) file.
11. Optionally enter the **Description**.
12. Click **Save**.

    The new report is listed under **PDF/XLS Reports** tab (**Report Templates** tab starting with Oracle AVDF release 20.8).

> **See Also:**
>
> - Accessing Your Saved Custom Reports
> - Related Event Data Appendices
> - Logging in to the Audit Vault Server Console
> - Oracle BI Publisher Documentation
> - Oracle Fusion Applications Administering Reports and Analytics Guide

8.10 Scheduling and Generating PDF or XLS Reports

Auditors can schedule and generate PDF or XLS reports.

8.10.1 About Scheduling and Creating PDF or XLS Reports

Auditors 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.

For Oracle AVDF 20.1 - 20.9, the timestamp shown in scheduled reports is based on the **Timezone Offset** setting specified by the user in the Audit Vault Server. See *Oracle Audit Vault and Database Firewall Administrator's Guide* for more information.

Starting in Oracle AVDF 20.10, the timestamp shown in scheduled reports is based on the **Timezone Offset** setting specified by an auditor in the **Report Schedules** tab or the **Schedule** icon in reports. This offset will only apply to report schedules and is independent of the Audit Vault Server console's timezone offset.

To schedule a saved interactive report, refer to Creating and Scheduling a Custom Report.

8.10.2 Creating a Report Schedule

When you create a report schedule, you can add filters such as a limit to the number of rows generated.

1. Log in to the Audit Vault Server as an *auditor*.
2. Click the **Reports** tab.
3. Find the report you want to schedule, and click on the icon under **Schedule**.
4. In the page displayed, under the **Schedule Report** section, select the **Report Format.** You can choose **PDF** or **XLS**.

   You can optionally change the **Report Name**. The **Category Name** field is already filled in and cannot be changed.
5. In the **Report Filters** section, enter or select:
   - **Target** - This appears if applicable to the report.
   - **Row Limit** - The maximum limit for this parameter (`ROW_LIMIT`) is `999999`.
   - **Event Time**
6. In the **Schedule** section, select how you want to schedule the report:
   - **Immediately** - Runs the report immediately.
   - **Specify Schedule** - Specify the time and date the report will begin to run and the repeat frequency.
   - **Select Schedule** - 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:**
   >
   > These 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.
7. In the **Retention Policy** section, if necessary, click on the edit icon to change the default archiving policy, and then click on the check mark.

   The archiving (or retention) policy is created by an Oracle Audit Vault and Database Firewall 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).
8. In the **Notification** section, optionally select users to notify about this report:

- For the **Send** field, select either **URL** 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 e-mail** and **Cc** fields. Enter full email addresses separated by commas.
- Click **Add to List.**

9. Under **Attestation** section, 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.

10. Click on the **Schedule** button at the top right corner of the page.

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

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

> **Note:**
>
> Avoid triggering or scheduling concurrent long running reports at the same time, as they may be left in a hung state forever. The reports must be scheduled with staggered intervals in between. For example, a gap of `5`, `10`, or `20` minutes.

> **See Also:**
>
> - *Oracle Audit Vault and Database Firewall Administrator's Guide* for more information on archiving policies.
> - Logging in to the Audit Vault Server Console
> - Creating or Modifying an Email Distribution List
> - Creating or Modifying an Email Distribution List

8.10.3 Viewing or Modifying Report Schedules

An auditor can view and modify scheduled reports.

To view or modify report schedules, navigate to the **Reports** tab, and then click on **Report Schedules** on the left navigation.

> **See Also:**
>
> Creating a Report Schedule for details on report schedule fields.

8.10.4 View and Edit All Scheduled Reports

Starting in Oracle AVDF 20.10, you can view all scheduled reports and adjust the time zone offset for all scheduled reports on the **Report Schedules** page.

1. Log in to the Audit Vault Server Console as an `auditor`.
2. Clicks the **Reports** tab.
3. Click on **Report Schedules**.
4. Click **Change** to adjust the time zone offset for all scheduled reports.
5. View the **Report Schedules** for all reports.

8.10.5 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.

The format in which you can download the report depends 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.

1. Log in to the Audit Vault Server as an *auditor*.
2. Click on the **Reports** tab.
3. Click on **Generated Reports** tab in the left navigation menu.

   A list of generated reports appear.
4. 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 on the report name, and then save the file.
   - To notify another user of the report, select the check box against the specific report, and then click **Notify**.
   - To attest and annotate the report, click the **Details** icon in the second column.

> **See Also:**
>
> - Downloading a Report in HTML or CSV Format
> - Logging in to the Audit Vault Server Console
> - Notifying Users About Generated PDF or XML Reports
> - Annotating and Attesting Reports

8.10.6 Notifying Users About Generated PDF or XML Reports

You can send notifications to other users or distribution lists about a scheduled and generated report.

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

2. Click on the **Reports** tab.
3. Click on the **Generated Reports** tab in the left navigation menu.

   A list of generated reports appear.
4. Select the check box for the specific report and then click the **Notify** button.
5. In the **Notification** section, perform the following:
   - For the **Send** field, select either **URL** 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 e-mail** and **Cc** fields. Enter full email addresses separated by commas.
6. Click **Notify**.

> **See Also:**
>
> Logging in to the Audit Vault Server Console

8.11 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.

1. Log in to the Audit Vault Server as an *auditor*.
2. Click the **Reports** tab.
3. Click the **Generated Reports** tab in the left navigation menu.
4. Click the **Details** icon of the specific report.
5. Scroll down to the **Attestations** section.
6. In the **Notes** field, enter a note for the report.
7. 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 download the report, click the **Download Report** button.
8. To return to the **Generated Reports** page, click the **Cancel** button.

   The Generated Reports page appears.

Related Topics

- Filtering Data in a Report
  You can filter the report to show data based on a search, a particular value, or an expression. Starting in Oracle AVDF 20.11, you can also filter the All Activity Report based on a Global Set, as well as filter Compliance GDPR Reports (including Sensitive Data, Access Rights to Sensitive Data, Activity on Sensitive Data, and Activity on Sensitive Data by Privileged Users) based on a Sensitive Objects Set.
- Logging in to the Audit Vault Server Console
  To log in to the Audit Vault Server console, you must have a valid user name and password.

8.12 Downloading a Report in HTML or CSV Format

You can download reports in `.csv` (for use in an Excel spreadsheet) or `html` format.

1. Log in to the Audit Vault Server console as an *auditor*.
2. Click the **Reports** tab.
3. All the report categories are listed in the left navigation menu. Select the specific report category. For example, click **Activity Reports** sub tab.
4. Select the specific report.
5. Use the filter options using the search field or by clicking on the column names. From the **Actions** menu, select **Download**.
6. Select **CSV** or **HTML** in the dialog.
7. In the opening dialog box, select **Save File** and then click **OK**.
8. Select a location and enter a name for the file.
9. Click **Save**.

> **See Also:**
>
> Logging in to the Audit Vault Server Console

8.13 Related Event Data Appendices

For audit data, reports track audit events from a variety of sources, such as Oracle Database audit events, Sybase ASE audit events, and so on.

See the following appendices for more information:

- Oracle Database Audit Events
- Sybase ASE Audit Events
- Microsoft SQL Server SQL Trace Audit Events
- Microsoft SQL Server SQL Audit and Event Log Events
- IBM DB2 Audit Events
- MySQL Audit Events
- Solaris Operating System Audit Events

- Microsoft Windows Operating System Audit Events
- Linux Operating System Audit Events
- Oracle ACFS Audit Events
- Active Directory Audit Events

9
Managing Entitlements

Learn about managing entitlements.

9.1 Managing and Viewing Entitlement Data

Oracle Audit Vault and Database Firewall provides default entitlement reports and allows you to retrieve entitlement data from Oracle Database 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* targets, if you are not using multitenant container databases (CDBs), then 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 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 target to create a snapshot of the data at that point in time.
2. Optionally, create labels to organize the snapshots into meaningful groups, and assign the labels to snapshots.
3. View entitlement reports, using snapshots and labels to filter and compare data.

> **See Also:**
>
> - Retrieving User Entitlement Data for Oracle Database Targets
> - Creating, Modifying, or Deleting Labels for Entitlement Snapshots
> - Assigning Labels to Entitlement Snapshots
> - Generating Entitlement Reports
> - Entitlement Report Descriptions

9.2 Working With Entitlement Snapshots and Labels

Learn about working with entitlement snapshots and labels.

9.2.1 About Entitlement Snapshots and Labels

An entitlement snapshot captures the state of user entitlement information at a specific point in time.

When you retrieve entitlement data from an Oracle Database target, a **snapshot** of that data is created, and added to the list in the User Entitlement Snapshots page in the **Targets** tab.

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 targets to which you have access.

Each snapshot is unique for a 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 targets at this time, then each 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 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 targets, together in the same report.

> **Note:**
>
> All user entitlement snapshots will be purged after 18 months from the time of data retrieval.

> **See Also:**
>
> Retrieving User Entitlement Data for Oracle Database Targets

9.2.2 Creating, Modifying, or Deleting Labels for Entitlement Snapshots

An auditor can create, modify, or delete labels for entitlement snapshots.

1. Log into the Audit Vault Server console as an *auditor*.
2. Click on **Targets** tab.
3. Click on **User Entitlement Snapshots** sub tab in the left navigation menu.
4. Click on **Labels** button in the top right corner of the main page.
5. The **Labels** dialog is displayed. In this dialog:
   - 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**.

> **See Also:**
>
> Logging in to the Audit Vault Server Console

9.2.3 Assigning Labels to Entitlement Snapshots

Before you can assign labels to snapshots, you must first retrieve entitlement data from an Oracle Database target.

This process creates a snapshot each time you do so.

1. Log into the Audit Vault Server console as an *auditor*.
2. Click on **Targets** tab.
3. Click on **User Entitlement Snapshots** sub tab in the left navigation menu.
4. 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.
5. To assign a label to snapshots:
   a. Select the snapshots, select the check box for the targets and then click **Assign Label**.
   b. Select a **Label** from the list.
   c. Optionally, enter a description.
   d. Click **Save**.
6. To delete a snapshot, select the snapshot, and then click **Delete**.

> **See Also:**
>
> - Retrieving User Entitlement Data for Oracle Database Targets
> - Working with Lists of Objects in the UI
> - Logging in to the Audit Vault Server Console

9.3 Generating Entitlement Reports

Learn about entitlement reports.

9.3.1 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 target (for example, User Accounts by Target) let you view and compare snapshots for a specific target. The other entitlement reports (such as User Accounts) let you view and compare entitlement data by label across all the targets.

9.3.2 Viewing Entitlement Reports by Snapshot or Label

An auditor can check entitlement reports for an individual snapshot or label.

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

   The **Activity Reports** sub tab in the left navigation menu is selected by default.
3. Scroll down in the main page and expand **Entitlement Reports**.
4. Click on a specific entitlement report.
5. In this page you can do the following:
   - If you want the report to be sorted by target, then select a target in the **Target Name** field.
   - From the **Snapshot** field, select the snapshot or label.
6. 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.
7. Optionally, you can save the report.

Related Topics

- Entitlement Reports
  The **Entitlement Reports** capture information such as a user's roles, object privileges, system privileges, and so on.
- Customizing Reports
  You can customize existing reports by using built-in tools to filter, group, and highlight data and define columns. These customized reports can be saved as new report formats and accessed from the **Saved Reports** tab. Saved custom formats of existing reports can only be viewed online as they can't be scheduled or printed in PDF format.
- Logging in to the Audit Vault Server Console
  To log in to the Audit Vault Server console, you must have a valid user name and password.

9.3.3 Comparing Entitlement Data Using Snapshots or Labels

An auditor can compare the entitlement data for two snapshots or labels.

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

   The **Activity Reports** sub tab in the left navigation menu is selected by default.
3. Scroll down in the main page and expand **Entitlement Reports**.
4. Click on a specific entitlement report.
5. In the report, do the following:

- If you want the report to be sorted by target, then select a target in the **Target Name** field.
- From the **Snapshot** field, select the snapshot or label.
- Click the **compare** check box.
- Select another snapshot or label from the second drop-down list for comparison.

6. Click **Go**.

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

> **See Also:**
>
> Logging in to the Audit Vault Server Console

9.4 Entitlement Report Descriptions

Learn about entitlement reports.

9.4.1 About the Entitlement Reports

An entitlement report describes the types of access that users have to an Oracle Database target.

It provides information about the user, role, profile, and privileges used in the 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 Also:**
>
> - Generating Entitlement Reports
> - Filtering Data in a Report
> - Generating Entitlement Reports for information about generating and viewing entitlement report data.
> - Customizing Reports for information about creating user-defined reports from entitlement reports.

9.4.2 Role Privileges

The Role Privileges report shows information about application roles and privileges.

Use this report to track the names of application roles and privileges. If the role is a secure application role, then the columns of the report indicate the same.

9.4.3 Object Privileges

The Object Privileges report shows object privileges and their grants to users.

Use these reports to track object privileges and their grants to users the following information about object privileges: the 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.

Columns Related to Oracle Database 12c

You can select these additional columns relating to Oracle 12c targets:

- Hierarchy: Privilege is with hierarchy option
- Type: Object type (table, view, sequence, and so on.)
- 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.

9.4.4 Privileged Users

The Privileged Users report shows information about privileged users.

Use these reports to track the following information about privileged users: 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:

```
DBA
SYSDBA
SYSOPER
```

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

```
SYSASM
SYSBACKUP
SYSDG
SYSKM
```

Columns Related to Oracle Database 12c

You can select these additional columns relating to Oracle 12c 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.

9.4.5 System Privileges

The System Privileges report shows system privileges and their grants to users.

Use these reports to track the following information about system privileges: 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.

Columns Related to Oracle Database 12c

You can select these additional columns relating to Oracle 12c 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.

9.4.6 User Accounts Reports

The User Accounts report shows a summary of user accounts.

Use these reports to track the following information about user accounts: 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).

Columns Related to Oracle Database 12c

You can select these additional columns relating to Oracle Database 12c 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.

9.4.7 User Privileges

The User Privileges report shows a summary of user privileges.

Use these reports to track the following information about user privileges: 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.

Columns Related to Oracle Database 12c

You can select these additional columns relating to Oracle 12c targets:

- Hierarchy: Privilege is with hierarchy option
- Type: Object type (table, view, sequence, and so on)
- 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.

9.4.8 User Profiles

The User Profiles report shows a summary of user profiles.

Use these reports to track the following information about user profiles: target in which the user profile was created, profile name, resource name, resource type (`KERNEL`, `PASSWORD`, or `INVALID`), and profile limit.

Columns Related to Oracle Database 12c

You can select these additional columns relating to Oracle 12c 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.

10 Creating Alerts

Learn about creating alerts.

10.1 About Alerts

You should understand how alerts work in general and how to define useful alerts.

10.1.1 Overview

Alerts can be used for targets and third-party plug-ins.

You can create and configure alerts on events for targets, and for third-party plug-ins that have been developed using the Oracle Audit Vault and Database Firewall 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 targets, such as four Oracle databases. The alert rule can include more than one event and the event comes from different targets. For example, User A failed to log in to target X and User A also failed to log in to target Y.

You can specify an alert severity. Also, if a 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.

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 records are collected. 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.

Alerts have a retention policy of three months online and zero months in archive.

Related Topics

- Oracle Database Audit Events
  Audit events are in a wide variety of categories, such as account management events and peer association events.
- Active Directory Audit Events
  Learn about Active Directory audit events.
- Database Firewall Policies
  You can create and manage Database Firewall policies.

- Alert Reports
  The alert reports track critical and warning alerts. The alerts report will only show alerts from the past three months, as alerts have a retention policy of three months online and zero months in archive.
- Creating Templates and Distribution Lists for Email Notifications
  Email templates and notifications help auditors to notify other users automatically about audit-related events.

10.1.2 Defining Useful Alerts

A good way to define meaningful alerts is to first browse activity reports in Oracle Audit Vault and Database Firewall.

Activity reports contain a variety of audit and network event data, so browsing them can help you determine the key fields in audit records that are of special interest to you. These audit record fields are columns in the activity reports.

Looking at the report columns of interest, and the values in those columns, is a useful starting point for creating an alert that focuses on the audit events on which you want to be alerted. You can then create an alert with a condition (a rule) that defines the specific audit record field(s) and values that will trigger the alert.

For example, suppose you want to be alerted on schema changes to certain database objects. You can start by browsing the Database Schema activity report.

In this report, you can see the various database target objects, users, client program names, and other data associated with schema change audit events captured by Oracle Audit Vault and Database Firewall. From here, you can decide which target objects you want to alert on. You can then narrow down the alert to specific users, client programs, etc.

Related Topics

- Activity Reports
  Learn about activity reports.

10.2 Creating Alerts and Writing Alert Conditions

Learn about creating alerts and writing alert conditions.

10.2.1 Creating or Modifying an Alert

You create custom alerts or use a predefined alert.

When you create an alert in Oracle Audit Vault and Database Firewall, 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, which will notify administrator Z, using a specific email notification template. Oracle Audit Vault and Database Firewall 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.

Tip:

Oracle recommends creating an alert policy with email notifications to monitor the AVREPORTUSER, AVSAUDIT, and ORDS_PUBLIC_USER users.
Create an alert policy with email notification with the following condition:

```
upper(:EVENT_STATUS)='FAILURE' and upper(:EVENT)='LOGON' and
(upper(:USER)='AVREPORTUSER' or upper(:USER)='AVSAUDIT' or
upper(:USER)='ORDS_PUBLIC_USER')
```

If you receive an alert you should check the event details and take action to prevent further login attempts for the AVREPORTUSER, AVSAUDIT, and ORDS_PUBLIC_USER users.

- Oracle AVDF Release 20.11 and later
- Oracle AVDF Release 20.1-20.10

Oracle AVDF Release 20.11 and later

1. Log in to the Audit Vault Server Console as an auditor.
2. Click on **Policies** tab.
3. From the left navigation menu, select **Alert Policies**.
4. To view or modify the definition for an existing alert, click its name in the **Alert Name** field.
5. To create a new alert definition click **Create**.
6. Enter the **Alert policy name**.
7. Specify the information in the following fields:
   - **Alert description:** Optionally, enter a description for this alert.
   - **Target type:** Select a target type. For example, Oracle Database.
   - **Severity:** Select **Warning** or **Critical**.
   - **Condition:** Enter a Boolean condition that must be met for this alert to be triggered.

     You can click any of the **Condition - Available Fields** listed on the right to enter them as part of the alert condition. These fields are the permissible audit or network event 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, making sure to include a **colon** (**:**) before that field. For example, your condition may be:

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

> **Caution:**
>
> Starting in Oracle AVDF 20.11 the following attributes have been changed:
>
> – The `COMMAND_CLASS` attribute can't use DML, DDL, or DCL. Instead, you must use specific commands such as `INSERT`, `UPDATE`, or `DELETE`. You will need to modify your existing alert policies to accommodate these changes. See Command Class to Command Mappings for Alert Policies and Reports for information on what commands to use.
>
> – The `EVENT` attribute can't use `session` or `statement` values. You will need to modify your existing alert policies to accommodate these changes. See Session or Statement to Command Mappings for Alert Policies and Reports for information on what commands to use.
>
> – The `CLUSTER_TYPE` attribute can't be used.

Starting in Oracle AVDF 20.11, users can add filters in the UI interactive report provided on the create alert policy and copy them in an alert condition. Underneath the **Condition** field, users can choose either **Copy condition from examples**, **Copy condition from alert policies**, **Create condition using report**, or **Create condition using global sets** (Oracle AVDF 20.13 and later).

For creating a condition from a global set, only one global set can be specified in a condition clause but additional global set conditions can be appended with `AND` or `OR`. The following table shows which alert fields will be checked depending on the selected global set.

Global Set	Alert Field
IP Address Set	CLIENT_IP
OS User Set	OSUSER
Client Program Set	CLIENT_PROGRAM
Database User Set	USER
Privileged User Set	USER
Sensitive Object Set	OBJECT

Related Topics

– All Activity Report

– Filtering by a Global Set in an All Activity Report

– Global Sets - Oracle AVDF 20.10 and later

8. Optionally, in the threshold condition area, specify the following information:

   - **Threshold (number):** Enter the number of times the alert condition should be met before the alert is raised.
   - **Duration (in minutes):** 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 met 3 times in 5 minutes to raise an alert.
   - **Group By (field):** Select a field from the list to group events by this column for this alert.

9. Optionally, in the **Configure email notification** area, specify the following information:
   a. **Enable email notification:**When email notifications are disabled, there is no other information needed. When email notifications are enabled, specify the following information:
      - **Email template:** Select a notification template to use for this alert. Starting in Oracle AVDF 20.11, users can associate only one notification template per alert policy. On an upgrade to 20.11, the alert notification template for an existing alert policy will be set to the default alert template.

        See Creating Templates and Distribution Lists for Email Notifications for more detailed information.
      - **To:** Enter email addresses to receive notifications by writing out the address, followed by the Enter key. Once an email address has been entered, then you can continue writing additional email addresses. In addition to email addresses, you can enter distribution lists directly into this field, followed by the Enter key. If you would like to create a distribution list, click the plus button and add the required information. Enter the Name and Email addresses desired for the list. You can also set this as your default distribution list for email notifications. Any distribution list that you have previously set as default will automatically populate this field.
      - **Cc:** Enter email addresses to be copied on notifications by writing out the address, followed by the Enter key. Once an email address has been entered, then you can continue writing additional email addresses. In addition to email addresses, you can enter distribution lists directly into this field, followed by the Enter key. If you would like to create a distribution list, click the plus button and add the required information. Enter the Name and Email addresses desired for the list.
10. Click **Save**.

    The new alert appears in the **Alert Policies** page.

Oracle AVDF Release 20.1-20.10

1. Log in to the Audit Vault Server Console as an `auditor`.
2. Click on **Policies** tab.
3. From the left navigation menu, select **Alert Policies**.
4. To view or modify the definition for an existing alert, click its name in the **Alert Name** field.
5. To create a new alert definition click **Create**.
6. Enter the **Alert Name**.
7. Specify the information in the following fields:
   - **Type:** Select a target type. For example, Oracle Database.
   - **Severity:** Select **Warning** or **Critical**.
   - **Threshold (times):** Enter the number of times the alert condition should be met before the alert is raised.
   - **Duration (min):** 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 met 3 times in 5 minutes to raise an alert.
   - **Group By (Field):** Select a field from the list to group events by this column for this alert.
   - **Description:** Optionally, enter a description for this alert.

- **Condition:** Enter a Boolean condition that must be met for this alert to be triggered.

  You can click any of the **Condition - Available Fields** listed on the right to enter them as part of the alert condition. These fields are the permissible audit or network event 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, making sure to include a **colon** (**:**) before that field. For example, your condition may be:

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

8. Optionally, in the **Notification** area, specify the following information:

   a. **Template:** Select a notification template to use for this alert.

   b. **Distribution List:** Select an email distribution list that will be notified about this alert.

   c. **To:** Enter email addresses, separated by commas, to receive notifications.

   d. **Cc:** Enter email addresses, separated by commas, to be copied on notifications.

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

9. Click **Save**.

   The new alert appears in the **Alert Policies** page.

You can monitor alert activity from the dashboard on the Audit Vault Server console **Home** page.

Related Topics

- Writing Alert Conditions
  Learn how to define alert conditions.
- Monitoring Alerts
  Oracle AVDF raises an alert when data matches an alert rule condition in a single audit record, or matches multiple events with its duration and threshold setting.

10.2.1.1 Command Class to Command Mappings for Alert Policies and Reports

Starting in Oracle AVDF 20.11, Database Firewall and Alert policies no longer utilize command classes. Instead, users are able to create policies based on specific commands such as `INSERT`, `UPDATE`, or `DELETE`. This table can help you identify which commands are a part of which command class.

Command Class	Commands for Oracle	Commands for SQL Server	Commands for MySQL	Commands for DB2 LUW	Commands for Sybase ASE
DCL	ADMINISTER, ALTER, CHANGE, COMPRESS, ENCRYPT, GRANT, INVALID, LOGIN, ORADEBUG, REVOKE, SET, STOP	ALTER, DENY, GRANT, LOGIN, REVOKE, SET, USE, VALIDATE	BINLOG, DROP, FLUSH, GRANT, INSTALL, KEYCACHE, KILL, LOAD, RESET, REVOKE, SET, UNINSTALL, USE	GRANT, REVOKE, SET, TRANSFER	EXECUTE, GRANT, KILL, LOAD, LOCK, MOUNT, REVOKE, SET, TRANSFER, USE, VALIDATE
DDL	ALTER, ANALYZE, ASSOCIATE, AUDIT, COMMENT, CREATE, DISASSOCIATE , DROP, NOAUDIT, RENAME, TRUNCATE	ADD, ALTER, CREATE, DISABLE, DROP, ENABLE, RECONFIGURE, TRUNCATE, USE	ALTER, CHECK, CHECKSUM, CREATE, DROP, PARTITION, RENAME, REPLACE, TRUNCATE	ALLOCATE, ALTER, COMMENT, CREATE, DROP, RENAME, TRUNCATE	ALTER, CREATE, DEALLOCATE, DROP, TRUNCATE
DML	DELETE, DROP, EXECUTE, EXPLAIN, INSERT, MERGE, RETRIEVE, UPDATE, WRITE	BACKUP, DELETE, INSERT, MERGE, RESTORE, UPDATE, WRITE	ANALYZE, DELETE, GET, INSERT, LOAD, OPTIMIZE, REPAIR, UPDATE	DELETE, EXPLAIN, INSERT, MERGE, REFRESH, UPDATE	DELETE, DUMP, EXECUTE, INPUT, INSERT, MERGE, QUIESCE, REFRESH, REMOVE, UNMOUNT, UPDATE, WRITE
Logon	LOGIN	LOGIN	LOGIN	LOGIN	LOGIN
Logoff	LOGOUT	LOGOUT	LOGOUT	LOGOUT	LOGOUT
Procedural	EXECUTE, EXIT, LOCK	CHECKPOINT, DEALLOCATE, END, EXECUTE, GET, KILL, LOAD, MOVE, PRINT, RECEIVE, REVERT, SEND, SLOWDOWN, STOP	CHANGE, DEALLOCATE, EXECUTE, PREPARE, RESIGNAL, SET, SIGNAL, START, STOP	ASSOCIATE, AUDIT, CONNECT, DECLARE, DISCONNECT, EXECUTE, FLUSH, FREE, GET, LOCK, PREPARE, RELEASE, RESIGNAL, SIGNAL	CHECKPOINT, CLEAR, CONFIGURE, CONNECT, DISCONNECT, EXECUTE, EXIT, OUTPUT, PREPARE, PRINT, PUBLISH, QUIT, RECONFIGURE, START, STOP

Command Class	Commands for Oracle	Commands for SQL Server	Commands for MySQL	Commands for DB2 LUW	Commands for Sybase ASE
Select	`SELECT`	`READ, SELECT`	`SELECT`	`DESCRIBE, SELECT, VALUES`	`SELECT`
Transaction	`COMMIT, ROLLBACK, SAVEPOINT, SET, TRANSACTION`	`BEGIN, COMMIT, ROLLBACK, SAVE, SET`	`COMMIT, END, LOCK, PREPARE, RECOVER, RELEASE, ROLLBACK, SAVEPOINT, START, UNLOCK`	`COMMIT, ROLLBACK, SAVEPOINT`	`COMMIT, ROLLBACK, SAVE, START`

10.2.1.2 Session or Statement to Command Mappings for Alert Policies and Reports

Starting in Oracle AVDF 20.11, Alert policies no longer utilize session or statement classes. Instead, users are able to create policies based on specific commands such as `INSERT`, `UPDATE`, or `DELETE`. This table can help you identify which commands are a part of which statement class.

Statement Class	Commands for Oracle	Commands for SQL Server	Commands for MySQL	Commands for DB2 LUW	Commands for Sybase ASE
DCL	ADMINISTER KEY MANAGEMENT, ALTER SESSION, ALTER SYSTEM, CHANGE PASSWORD, COMPRESSED, ENCRYPTED, GRANT OBJECT, GRANT ROLE, INVALID OPERATION, LOGIN, ORADEBUG, REVOKE OBJECT, REVOKE ROLE, SET ROLE, SHUTDOWN	ALTER AUTHORIZATION, DBCC, DENY, GRANT, LOGIN, REVOKE, SET, SETUSER, USE DATABASE	BINLOG, FLUSH, GRANT, INSTALL, KEYCACHE, KILL, LOAD INDEX, PURGE, RESET, REVOKE, SET ROLE, UNINSTALL, USE	GRANT, REVOKE, SET, TRANSFER	DBCC ADDTEMPDB, DBCC CHECKALLOC, DBCC CHECKCATALOG, DBCC CHECKDB, DBCC CHECKINDEX, DBCC CHECKSTORAGE, DBCC CHECKTABLE, DBCC CHECKVERIFY, DBCC COMPLETE XACT, DBCC DBREPAIR, DBCC ENGINE, DBCC FIX TEXT, DBCC FORGET XACT, DBCC INDEXALLOC, DBCC MONITOR, DBCC NODETRACEOFF, DBCC NODETRACEON, DBCC PRAVAILABLETEMPDBS, DBCC QUORUM, DBCC REBUILD TEXT, DBCC REINDEX, DBCC SERVERLIMITS, DBCC SET SCOPE, DBCC SHRINKDB SETUP, DBCC STACKUSED, DBCC TABLEALLOC, DBCC TEXTALLOC, DBCC TRACEOFF, DBCC TRACEON,

Statement Class	Commands for Oracle	Commands for SQL Server	Commands for MySQL	Commands for DB2 LUW	Commands for Sybase ASE
					DBCC TUNE, DBCC UPGRADE OBJECT, DBCC ZAPDEFRAGINFO, GRANT, KILL, LOAD DATABASE, LOAD TRANSACTION, LOCK TABLE, MOUNT DATABASE, REVOKE, SET, SETUSER, SYSTEM, TRANSFER TABLE, USE

Statement Class	Commands for Oracle	Commands for SQL Server	Commands for MySQL	Commands for DB2 LUW	Commands for Sybase ASE
DDL	ALTER ANALYTIC VIEW, ALTER ATTRIBUTE DIMENSION, ALTER AUDIT POLICY, ALTER CLUSTER, ALTER DATABASE, ALTER DATABASE DICTIONARY, ALTER DATABASE LINK, ALTER DIMENSION, ALTER DISKGROUP, ALTER FLASHBACK ARCHIVE, ALTER FUNCTION, ALTER HIERARCHY, ALTER INDEX, ALTER INDEXTYPE, ALTER INMEMORY JOIN GROUP, ALTER JAVA, ALTER LIBRARY, ALTER LOCKDOWN PROFILE, ALTER MATERIALIZED VIEW, ALTER MATERIALIZED VIEW LOG, ALTER MATERIALIZED ZONEMAP, ALTER OPERATOR, ALTER OUTLINE, ALTER PACKAGE, ALTER	ADD SIGNATURE, ALTER APPLICATION, ALTER ASSEMBLY, ALTER ASYMMETRIC KEY, ALTER AVAILABILITY GROUP, ALTER BROKER PRIORITY, ALTER CERTIFICATE, ALTER COLUMN ENCRYPTION KEY, ALTER CREDENTIAL, ALTER CRYPTOGRAPHIC PROVIDER, ALTER DATABASE, ALTER DATABASE AUDIT, ALTER DATABASE KEY, ALTER DATABASE SCOPED CONFIGURATION, ALTER DATABASE SCOPED CREDENTIAL, ALTER ENDPOINT, ALTER EVENT SESSION, ALTER EXTERNAL DATA SOURCE, ALTER EXTERNAL LANGUAGE, ALTER EXTERNAL LIBRARY, ALTER EXTERNAL RESOURCE POOL, ALTER FEDERATION,	ALTER DATABASE, ALTER EVENT, ALTER FUNCTION, ALTER INSTANCE, ALTER LOGFILE, ALTER PROCEDURE, ALTER SERVER, ALTER TABLE, ALTER TABLESPACE, ALTER USER, ALTER VIEW, CHECK, CHECKSUM, CREATE DATABASE, CREATE EVENT, CREATE FUNCTION, CREATE INDEX, CREATE LOGFILE, CREATE PROCEDURE, CREATE ROLE, CREATE SERVER, CREATE TABLE, CREATE TABLESPACE, CREATE TRIGGER, CREATE USER, CREATE USER FUNCTION, CREATE VIEW, DROP DATABASE, DROP EVENT, DROP FUNCTION, DROP INDEX, DROP PROCEDURE, DROP ROLE,	ALLOCATE, ALTER AUDIT POLICY, ALTER BUFFERPOOL, ALTER DATABASE, ALTER EVENT, ALTER FUNCTION, ALTER HISTOGRAM, ALTER INDEX, ALTER MASK, ALTER METHOD, ALTER MODULE, ALTER NICKNAME, ALTER NODEGROUP, ALTER PACKAGE, ALTER PERMISSION, ALTER PROCEDURE, ALTER SCHEMA, ALTER SECURITY, ALTER SEQUENCE, ALTER SERVER, ALTER SERVICE, ALTER SPECIFIC PROCEDURE, ALTER STOGROUP, ALTER TABLE, ALTER TABLESPACE, ALTER THRESHOLD, ALTER TRIGGER, ALTER TRUSTED CONTEXT, ALTER TYPE,	ALTER ALL, ALTER DATABASE, ALTER DEFAULT, ALTER ENCRYPTION KEY, ALTER FUNCTION, ALTER INDEX, ALTER LOGIN, ALTER MATERIALIZED VIEW, ALTER PRECOMPUTED RESULT SET, ALTER PROCEDURE, ALTER ROLE, ALTER RULE, ALTER TABLE, ALTER THREAD POOL, ALTER TYPE, ALTER VIEW, CREATE ARCHIVE DATABASE, CREATE DATABASE, CREATE DEFAULT, CREATE ENCRYPTION KEY, CREATE EXISTING TABLE, CREATE FUNCTION, CREATE INDEX, CREATE LOGIN, CREATE MATERIALIZED VIEW, CREATE PLAN, CREATE PRECOMPUTED RESULT SET, CREATE PROCEDURE, CREATE PROXY TABLE, CREATE ROLE, CREATE RULE,

Statement Class	Commands for Oracle	Commands for SQL Server	Commands for MySQL	Commands for DB2 LUW	Commands for Sybase ASE
	PLUGGABLE DATABASE, ALTER PROCEDURE, ALTER PROFILE, ALTER RESOURCE COST, ALTER ROLE, ALTER ROLLBACK SEGMENT, ALTER SEQUENCE, ALTER SYNONYM, ALTER TABLE, ALTER TABLESPACE, ALTER TRIGGER, ALTER TYPE, ALTER USER, ALTER VIEW, ANALYZE, ASSOCIATE, AUDIT, AUDIT CONTEXT, AUDIT POLICY, COMMENT, CREATE ANALYTIC VIEW, CREATE ATTRIBUTE DIMENSION, CREATE AUDIT POLICY, CREATE CLUSTER, CREATE CONTEXT, CREATE CONTROLFILE, CREATE DATABASE, CREATE DATABASE LINK, CREATE DIMENSION, CREATE DIRECTORY, CREATE DISKGROUP,	ALTER FULLTEXT, ALTER FUNCTION, ALTER INDEX, ALTER LOGIN, ALTER MASTER KEY, ALTER MESSAGE TYPE, ALTER PARTITION FUNCTION, ALTER PARTITION SCHEME, ALTER PROCEDURE, ALTER QUEUE, ALTER REMOTE, ALTER RESOURCE, ALTER ROLE, ALTER ROUTE, ALTER SCHEMA, ALTER SEARCH PROPERTY LIST, ALTER SECURITY POLICY, ALTER SEQUENCE, ALTER SERVER, ALTER SERVER CONFIGURATION, ALTER SERVER ROLE, ALTER SERVICE, ALTER SERVICE MASTER KEY, ALTER SYMMETRIC, ALTER TABLE, ALTER TRIGGER, ALTER USER, ALTER VIEW, ALTER WORKLOAD GROUP, ALTER	DROP SERVER, DROP TABLE, DROP TABLESPACE, DROP TRIGGER, DROP USER, DROP VIEW, PARTITION, RENAME TABLE, RENAME TABLES, RENAME USER, REPLACE, TRUNCATE TABLE	ALTER USAGE LIST, ALTER USER, ALTER VIEW, ALTER WORK, ALTER WORKLOAD, ALTER WRAPPER, ALTER XSROBJECT, COMMENT, CREATE ALIAS, CREATE AUDIT, CREATE BUFFERPOOL, CREATE DATABASE, CREATE DATABASE PARTITION GROUP, CREATE EVENT MONITOR, CREATE FUNCTION, CREATE GLOBAL TEMPORARY TABLE, CREATE HISTOGRAM, CREATE INDEX, CREATE MASK, CREATE METHOD, CREATE MODULE, CREATE NICKNAME, CREATE NODEGROUP, CREATE PERMISSION, CREATE PROCEDURE, CREATE ROLE, CREATE SCHEMA, CREATE SECURITY LABEL,	CREATE SCHEMA, CREATE SERVICE, CREATE TABLE, CREATE THREAD POOL, CREATE TRIGGER, CREATE VIEW, DEALLOCATE CURSOR, DEALLOCATE LOCATOR, DROP DATABASE, DROP DEFAULT, DROP ENCRYPTION KEY, DROP FUNC, DROP FUNCTION, DROP INDEX, DROP LOGIN, DROP LOGIN PROFILE, DROP MATERIALIZED VIEW, DROP PRECOMPUTED RESULT SET, DROP PROC, DROP PROCEDURE, DROP ROLE, DROP RULE, DROP SERVICE, DROP TABLE, DROP THREAD POOL, DROP TRIGGER, DROP VIEW, TRUNCATE LOB, TRUNCATE MATERIALIZED VIEW, TRUNCATE PRECOMPUTED RESULT SET,

Statement Class	Commands for Oracle	Commands for SQL Server	Commands for MySQL	Commands for DB2 LUW	Commands for Sybase ASE
	CREATE EDITION, CREATE FLASHBACK ARCHIVE, CREATE FUNCTION, CREATE HIERARCHY, CREATE INDEX, CREATE INDEXTYPE, CREATE INMEMORY JOIN GROUP, CREATE JAVA, CREATE LIBRARY, CREATE LOCKDOWN PROFILE, CREATE MATERIALIZED VIEW, CREATE MATERIALIZED VIEW LOG, CREATE MATERIALIZED ZONEMAP, CREATE OPERATOR, CREATE OUTLINE, CREATE PACKAGE, CREATE PACKAGE BODY, CREATE PFILE, CREATE PLUGGABLE DATABASE, CREATE PROCEDURE, CREATE PROFILE, CREATE RESTORE POINT, CREATE ROLE, CREATE ROLLBACK, CREATE	XML, CREATE AGGREGATE, CREATE APPLICATION, CREATE ASSEMBLY, CREATE ASYMMETRIC KEY, CREATE AVAILABILITY GROUP, CREATE BROKER PRIORITY, CREATE CERTIFICATE, CREATE COLUMN ENCRYPTION KEY, CREATE COLUMN MASTER KEY, CREATE COLUMNSTORE INDEX, CREATE CONTRACT, CREATE CREDENTIAL, CREATE CRYPTOGRAPHIC PROVIDER, CREATE DATABASE, CREATE DATABASE AUDIT, CREATE DATABASE KEY, CREATE DATABASE SCOPED CREDENTIAL, CREATE DEFAULT, CREATE DIAGNOSTICS SESSION, CREATE ENDPOINT, CREATE EVENT NOTIFICATION, CREATE EVENT		CREATE SECURITY POLICY, CREATE SEQUENCE, CREATE SERVER, CREATE SERVICE, CREATE SPECIFIC METHOD, CREATE STOGROUP, CREATE SYNONYM, CREATE TABLE, CREATE TABLESPACE, CREATE THRESHOLD, CREATE TRANSFORM, CREATE TRIGGER, CREATE TRUSTED CONTEXT, CREATE TYPE, CREATE USAGE LIST, CREATE USER, CREATE VARIABLE, CREATE VIEW, CREATE WORK, CREATE WORKLOAD, CREATE WRAPPER, DROP ALIAS, DROP AUDIT POLICY, DROP BUFFERPOOL, DROP DATABASE PARTITION GROUP, DROP EVENT MONITOR, DROP FUNCTION MAPPING, DROP	TRUNCATE TABLE

Statement Class	Commands for Oracle	Commands for SQL Server	Commands for MySQL	Commands for DB2 LUW	Commands for Sybase ASE
	SCHEMA, CREATE SEQUENCE, CREATE SPFILE, CREATE SYNONYM, CREATE TABLE, CREATE TABLESPACE, CREATE TRIGGER, CREATE TYPE, CREATE TYPE BODY, CREATE USER, CREATE VIEW, DISASSOCIATE, DROP ANALYTIC VIEW, DROP ATTRIBUTE DIMENSION, DROP AUDIT POLICY, DROP CLUSTER, DROP CONTEXT, DROP DATABASE, DROP DATABASE LINK, DROP DIMENSION, DROP DIRECTORY, DROP DISKGROUP, DROP EDITION, DROP FLASHBACK, DROP FUNCTION, DROP HIERARCHY, DROP INDEX, DROP INDEXTYPE, DROP INMEMORY JOIN GROUP, DROP JAVA,	SESSION, CREATE EXTERNAL DATA SOURCE, CREATE EXTERNAL FILE FORMAT, CREATE EXTERNAL LANGUAGE, CREATE EXTERNAL LIBRARY, CREATE EXTERNAL RESOURCE POOL, CREATE EXTERNAL TABLE, CREATE FEDERATION, CREATE FULLTEXT, CREATE FUNCTION, CREATE INDEX, CREATE LOGIN, CREATE MASTER KEY, CREATE MESSAGE TYPE, CREATE PARTITION, CREATE PROCEDURE, CREATE QUEUE, CREATE REMOTE, CREATE RESOURCE, CREATE ROLE, CREATE ROUTE, CREATE RULE, CREATE SCHEMA, CREATE SEARCH PROPERTY LIST, CREATE SECURITY		HISTOGRAM, DROP INDEX, DROP INDEX EXTENSION, DROP MASK, DROP METHOD, DROP MODULE, DROP NICKNAME, DROP NODEGROUP, DROP PACKAGE, DROP PERMISSION, DROP PROCEDURE, DROP ROLE, DROP SCHEMA, DROP SECURITY LABEL, DROP SECURITY POLICY, DROP SEQUENCE, DROP SERVER, DROP SPECIFIC PROCEDURE, DROP STOGROUP, DROP TABLE, DROP TABLESPACE(S), DROP THRESHOLD, DROP TRANSFORM(S), DROP TRIGGER, DROP TRUSTED CONTEXT, DROP TYPE, DROP USAGE LIST, DROP USER, DROP VARIABLE, DROP VIEW, DROP WORK, DROP WORKLOAD, DROP WRAPPER, DROP	

Statement Class	Commands for Oracle	Commands for SQL Server	Commands for MySQL	Commands for DB2 LUW	Commands for Sybase ASE
	DROP LIBRARY, DROP LOCKDOWN PROFILE, DROP MATERIALIZED VIEW, DROP MATERIALIZED VIEW LOG, DROP MATERIALIZED ZONEMAP, DROP OPERATOR, DROP OUTLINE, DROP PACKAGE, DROP PLUGGABLE DATABASE, DROP PROCEDURE, DROP PROFILE, DROP RESTORE, DROP ROLE, DROP ROLLBACK, DROP SEQUENCE, DROP SYNONYM, DROP TABLE, DROP TABLESPACE, DROP TRIGGER, DROP TYPE, DROP TYPE BODY, DROP USER, DROP VIEW, NOAUDIT, NOAUDIT CONTEXT, NOAUDIT POLICY, RENAME, TRUNCATE CLUSTER,	POLICY, CREATE SEQUENCE, CREATE SERVER, CREATE SERVER ROLE, CREATE SERVICE, CREATE STATISTICS, CREATE SYMMETRIC KEY, CREATE SYNONYM, CREATE TABLE, CREATE TRIGGER, CREATE TYPE, CREATE USER, CREATE VIEW, CREATE WORKLOAD GROUP, CREATE XML, DISABLE TRIGGER, DROP AGGREGATE, DROP APPLICATION, DROP ASSEMBLY, DROP ASYMMETRIC, DROP AVAILABILITY GROUP, DROP BROKER PRIORITY, DROP CERTIFICATE, DROP COLUMN ENCRYPTION KEY, DROP COLUMN MASTER KEY, DROP CONTRACT, DROP CREDENTIAL, DROP CRYPTOGRAPHI		XSROBJECT, RENAME INDEX, RENAME STOGROUP, RENAME TABLESPACE, TRUNCATE	

Statement Class	Commands for Oracle	Commands for SQL Server	Commands for MySQL	Commands for DB2 LUW	Commands for Sybase ASE
	TRUNCATE TABLE	C PROVIDER, DROP DATABASE, DROP DATABASE AUDIT, DROP DATABASE KEY, DROP DATABASE SCOPED CREDENTIAL, DROP DEFAULT, DROP DIAGNOSTICS SESSION, DROP ENDPOINT, DROP EVENT NOTIFICATION, DROP EVENT SESSION, DROP EXTERNAL DATA SOURCE, DROP EXTERNAL FILE FORMAT, DROP EXTERNAL LANGUAGE, DROP EXTERNAL LIBRARY, DROP EXTERNAL TABLE, DROP FEDERATION, DROP FULLTEXT CATALOG, DROP FULLTEXT INDEX, DROP FULLTEXT STOPLIST, DROP FUNCTION, DROP INDEX, DROP LOGIN, DROP MASTER KEY, DROP MESSAGE, DROP			

Statement Class	Commands for Oracle	Commands for SQL Server	Commands for MySQL	Commands for DB2 LUW	Commands for Sybase ASE
		PARTITION FUNCTION, DROP PARTITION SCHEME, DROP PROCEDURE, DROP QUEUE, DROP REMOTE, DROP RESOURCE, DROP ROLE, DROP ROUTE, DROP RULE, DROP SCHEMA, DROP SEARCH PROPERTY LIST, DROP SECURITY POLICY, DROP SEQUENCE, DROP SERVER, DROP SERVER ROLE, DROP SERVICE, DROP SIGNATURE, DROP STATISTICS, DROP SYMMETRIC, DROP SYNONYM, DROP TABLE, DROP TRIGGER, DROP TYPE, DROP USER, DROP VIEW, DROP WORKLOAD GROUP, DROP XML, ENABLE TRIGGER, RECONFIGURE, TRUNCATE, USE FEDERATION			

Statement Class	Commands for Oracle	Commands for SQL Server	Commands for MySQL	Commands for DB2 LUW	Commands for Sybase ASE
DML	`DELETE, EXECUTE CURSOR, EXPLAIN PLAN, FLASHBACK DATABASE, FLASHBACK TABLE, INSERT, LOB WRITE, MERGE, PURGE DBA RECYCLEBIN, PURGE INDEX, PURGE RECYCLEBIN, PURGE TABLE, PURGE TABLESPACE, UPDATE`	`BACKUP, DELETE, INSERT, INSERT BULK, MERGE, RESTORE, RESTORE DATABASE, UPDATE, UPDATE STATISTICS, UPDATETEXT, WRITETEXT`	`ANALYZE, DELETE, GET DIAGNOSTICS, INSERT, LOAD DATA, LOAD XML, OPTIMIZE, REPAIR, UPDATE`	`DELETE, EXPLAIN, INSERT, MERGE, REFRESH TABLE, UPDATE`	`DELETE, DUMP CONFIGURATION, DUMP DATABASE, DUMP TRANSACTION, EXECUTE CURSOR, INPUT, INSERT, MERGE, QUIESCE DATABASE, REFRESH PRECOMPUTED RESULT SET, REMOVE JAVA CLASS, REMOVE JAVA JAR, REMOVE JAVA PACKAGE, REORG COMPACT, REORG DEFRAG, REORG FORWARDED ROWS, REORG REBUILD, REORG RECLAIM SPACE, UNMOUNT DATABASE, UPDATE, WRITETEXT`
Logon	`LOGIN ATTEMPTED, LOGIN ATTEMPTED AND SUCCEDED, LOGIN FAILED`	`LOGIN ATTEMPTED, LOGIN ATTEMPTED AND SUCCEDED, LOGIN FAILED`	`LOGIN ATTEMPTED, LOGIN ATTEMPTED AND SUCCEDED, LOGIN FAILED`	`LOGIN ATTEMPTED, LOGIN ATTEMPTED AND SUCCEDED, LOGIN FAILED`	`LOGIN ATTEMPTED, LOGIN ATTEMPTED AND SUCCEDED, LOGIN FAILED`
Logoff	`LOGOUT`	`LOGOUT`	`LOGOUT`	`LOGOUT`	`LOGOUT`

Statement Class	Commands for Oracle	Commands for SQL Server	Commands for MySQL	Commands for DB2 LUW	Commands for Sybase ASE
Procedural	ASSIGNMENT, BEGIN, CALL ODBC, CASE, CLOSE, CONTINUE, DECLARE, EXEC, EXECUTE, EXECUTE IMMEDIATE, EXIT, FETCH, FOR, FORALL, FUNCTION, GOTO, IF, LOCK TABLE, LOOP, NULL, OPEN, OPEN FOR, PIPE, PLSQL BLOCK, PRAGMA AUTONOMOUS TRANSACTION, PROCEDURE, RAISE, RETURN, WHILE	BEGIN, BREAK, CALL, CHECKPOINT, CLOSE, CONTINUE, DEALLOCATE, DECLARE, END CONVERSATION , EXEC, EXECUTE, EXECUTE PROCEDURE, FETCH, GET CONVERSATION GROUP, GOTO, IF, KILL, LOAD, MOVE CONVERSATION , NULL, OPEN, PRINT, RAISEERROR, RECEIVE, RETURN, REVERT, RPC, SEND, SHUTDOWN, SLOWDOWN, THROW, WAIT FOR, WHILE	BEGIN, CALL, CASE, CHANGE, CLOSE, DEALLOCATE, DECLARE CONDITION, DECLARE CURSOR, DECLARE HANDLER, DECLARE VAR, DO, EXECUTE, FETCH, IF, ITERATE, LEAVE, LOOP, PREPARE, REPEAT, RESIGNAL, RETURN, SET VARIABLE, SIGNAL, START SLAVE, STOP SLAVE, WHILE	ASSIGNMENT, ASSOCIATE, AUDIT, BEGIN, CALL, CASE, CLOSE, CONNECT, DECLARE CURSOR, DECLARE GLOBAL TEMPORARY TABLE, DISCONNECT, EXECUTE, FETCH, FLUSH, FOR, FREE, GET, GOTO, IF, ITERATE, LEAVE, LOCK, LOOP, NULL, OPEN, PREPARE, RELEASE, REPEAT, RESIGNAL, RETURN, SIGNAL, WHILE	BEGIN, BREAK, CALL PROCEDURE, CALL SYSTEM PROCEDURE, CHECKPOINT, CLEAR, CLOSE, CONFIGURE, CONNECT, CONTINUE, DECLARE, DECLARE CURSOR, DISCONNECT, DISK, EXECUTE PROCEDURE, EXIT, FETCH, GO, GOTO, IF, ONLINE DATABASE, OPEN, OUTPUT, PARAMETERS, PREPARE DATABASE, PREPARE TRANSACTION, PRINT, QUIT, RAISERROR, RECONFIGURE, RETURN, RPC, SHUTDOWN, START LOGGING, STOP LOGGING, WAITFOR, WHILE
Select	DESCRIBE, LOB READ, SELECT	READTEXT, SELECT	DESCRIBE, EXPLAIN, HANDLER CLOSE, HANDLER OPEN, HANDLER READ, HELP, SELECT, SHOW	DESCRIBE, SELECT, VALUES	READ, READTEXT, SELECT

Statement Class	Commands for Oracle	Commands for SQL Server	Commands for MySQL	Commands for DB2 LUW	Commands for Sybase ASE
Transaction	`COMMIT, ROLLBACK, SAVEPOINT, SET CONSTRAINT, SET TRANSACTION, TRANSACTION`	`BEGIN TRANSACTION, COMMIT TRANSACTION, COMMIT WORK, ROLLBACK TRANSACTION, ROLLBACK WORK, SAVE TRANSACTION, SET TRANSACTION`	`BEGIN WORK, COMMIT, LOCK, RELEASE SAVEPOINT, ROLLBACK, SAVEPOINT, START TRANSACTION, UNLOCK, XA COMMIT, XA END, XA PREPARE, XA RECOVER, XA ROLLBACK, XA START`	`COMMIT, ROLLBACK, SAVEPOINT`	`BEGIN TRANSACTION, COMMIT, ROLLBACK, SAVE TRANSACTION`

10.2.2 Writing Alert Conditions

Learn how to define alert conditions.

10.2.2.1 About Alert Conditions

Learn about alert conditions.

The Alert Condition is the `where` clause of a select statement. In the **Condition** field of the Create Alert page, you can construct a Boolean condition that evaluates audit events. When the Boolean condition evaluates to `TRUE`, then Oracle Audit Vault and Database Firewall 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.

10.2.2.2 Writing an Alert Condition

Learn how to write an alert condition.

Syntax of Alert Conditions

The syntax for an alert condition is:

```
:condition_field operator expression
```

For example:

```
:event_status='FAILURE' and upper(:event_name)=upper('LOGON')
```

An alert condition is a `WHERE` clause in a `SELECT` statement, with an added **colon** (**:**) before the fields. For example, the above condition looks like the `WHERE` clause in this `SELECT` statement:

```
SELECT user_name, event_status, event_name from avsys.event_log
   WHERE event_status='FAILURE' and upper(event_name)=upper('LOGON');
```

The `WHERE` clause above captures events in the `avsys.event_log` table where the event was `LOGON` and the event status was `FAILURE`. Converting this `WHERE` clause to an alert condition will cause that alert to be triggered whenever there are failed logons. You can specify in the alert how many failed logons within a specified period of time trigger the alert.

Rules for Writing Alert Conditions

Table 10-1 lists the rules for writing alert conditions and gives some examples.

Table 10-1 Rules for Writing Alert Conditions

Use the available audit record fields	**The Create Alert page has a list of fields you can copy and use to build the alert condition. See Table 10-2.**
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, you can use: • `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 Audit Vault and Database Firewall 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 1	You want to be alerted whenever there are three failed logon attempts on Oracle Database targets within a five-minute period. To write a condition for this alert, you can copy EVENT_STATUS and EVENT_NAME from the available fields list, and use them to write this condition: `upper(:EVENT_STATUS)='FAILURE' and upper(:EVENT_NAME)='LOGON'` **Tip:** Set the threshold to 3 (3 times) and duration to 5 (less than 5 minutes) with this condition. You can look up audit event names and attributes in Oracle Database Audit Events.

Table 10-1 (Cont.) Rules for Writing Alert Conditions

Use the available audit record fields	The Create Alert page has a list of fields you can copy and use to build the alert condition. See Table 10-2.
Example 2	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." **Tip:** You can look up audit event names and attributes in Oracle Database Audit Events.

Alert for Example 1 (mentioned above) in the Audit Vault Server Console

This alert says: "Alert me whenever there are three failed logon attempts on Oracle Database targets within a five-minute period."

The alert **Condition** uses two of the **Condition - Available Fields** on the right side of the Create Alert page.

If this alert is raised, its **Severity** will be set to **Warning**. An email will also be sent to the user `avdf_auditor@samplecompany.com`, using the Alert Notification Template.

In reports, instances of this alert will be grouped by client application ID.

Available Audit Record Fields for use in Alert Conditions

Table 10-2 describes the available audit record fields you can use in alert conditions.

Important: These fields must be preceded by a colon (**:**) when used in the condition (for example `:USER_NAME`).

Table 10-2 Available Fields for Alert Conditions

Condition Field	Description
ACTION_TAKEN	(Firewall Alerts) Action taken by the Database Firewall, for example: `BLOCK`, `WARN`, or `PASS`
COLLECTION_TIME	The time Oracle Audit Vault and Database Firewall raised the alert
CLIENT_HOST	The host name of the client application that was the source of the event causing the alert
CLIENT_ID	The ID 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

Table 10-2   (Cont.) Available Fields for Alert Conditions

Condition Field	Description

CLUSTER_TYPE
Note:
Can only be used prior to AVDF 20.11
	(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 Starting in Oracle AVDF 20.11, the `COMMAND_CLASS` attribute can't use DML, DDL, or DCL. Instead, you must use specific commands such as `INSERT`, `UPDATE`, or `DELETE`. You will need to modify your existing alert policies to accommodate these changes. See Statement Class to Command Mappings for Database Firewall Policies for information on what commands to use.	The Oracle Audit Vault and Database Firewall command class. **Tip:** You can look up audit event names and attributes in Oracle Database Audit Events.
ERROR_CODE	The target's error code
ERROR_MESSAGE	The target's error message
EVENT	The target's audit event name. **Tip:** You can look up audit event names and attributes in Oracle Database Audit Events.
EVENT_STATUS	Status of the event: `Success` or `Failure`
EVENT_TIME	The time that the event occurred

LOCATION	Describes where the audit trail is located. Valid values are:
	`Audit File`
	`Audit Table`
	`Transaction Log`
	`Event Log`
	`Syslog`
	`Network`
	`Custom`

Table 10-2 (Cont.) Available Fields for Alert Conditions

Condition Field	Description
NETWORK_CONNECTION	Description of the connection between the 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
POLICY_NAME	The name of the Database Firewall policy or audit policy that generated this event. For Oracle AVDF 20.3 and later: In case of audit data collected by the Agent, the policy name contains the audit policies that caused the current event.
REPOSITORY_NAME	The name of the Container Database
ROW_COUNT	The number of rows returned by a SELECT DML query. **Note:** To fetch the row count, create a Database Object rule in a Database Firewall policy on the target. See Database Object Rule for more information.
OSUSER	Name of the target's OS user
TARGET_CLASS	Targets fall into these classes: Database OS Directory Service Filesystem
TARGET	Name of the target in Oracle Audit Vault and Database Firewall.
OBJECT	Name of the object on the target, for example, a table name, file name, or a directory name. Must be in upper case, for example, ALERT_TABLE.
OBJECT_OWNER	Owner of the object on the target
OBJECT_TYPE	The object type on the target, for example, TABLE, or DIRECTORY
TERMINAL	The Unix terminal that was the source of the event causing the alert (for example, /dev/1)
THREAT_SEVERITY	(Firewall Alerts) The threat severity of the SQL statement triggering the alert, as defined in a Database Firewall policy. Values may be: Minimal, Minor, Moderate, Major, or Critical.
USER	User name of the target user
AUDIT_TYPE Oracle AVDF 20.3 and later	Audit types for Oracle Database target: • Standard • FineGrainedAudit • XS • Database Vault • Label Security • RMAN_AUDIT • Datapump • Direct path API
APPLICATION_CONTEXT Oracle AVDF 20.3 and later	Application context information.

Table 10-2 (Cont.) Available Fields for Alert Conditions

Condition Field	Description
DATABASE_NAME Oracle AVDF 20.4 and later	The name of the DB2 database that contains the audit records.
INSTANCE_NAME Oracle AVDF 20.4 and later	The name of the instance which hosts the DB2 database.
RULE_NAME Oracle AVDF 20.5 and later	The name of the rule defined by the user in Database Firewall policy.

See Also:

- Oracle Database Audit Events

10.2.3 Disabling, Enabling, or Deleting Alerts

Learn how to enable, disable, or delete 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*.
2. Click on **Policies** tab.
3. From the left navigation menu, click **Alert Policies**. The alerts list is displayed on the main page.
4. Select the check box(es) to the left of the **Alert Name** column for the specific alerts. Click the **Disable**, **Enable**, or **Delete** button to perform that action on all selected alerts.

See Also:

- Working with Lists of Objects in the UI
- Logging in to the Audit Vault Server Console

10.3 Monitoring Alerts

Oracle AVDF raises an alert when data matches an alert rule condition in a single audit record, or matches multiple events with its duration and threshold setting.

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). Clicking on the circle marker available on the line chart will redirect you to **Alert Reports** under the **Alerts** tab.

You can also schedule alert reports from the Audit Vault Server **Reports** tab.

> **See Also:**
>
> - Alert Reports
> - Scheduling and Generating PDF or XLS Reports

10.4 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.

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

   A table of alerts can be seen. The table contains information regarding:

   - **Alert ID**
   - **Alert Status**
   - **Alert Policy**
   - **Target**
   - **User**
   - **Event**
   - **Object**
   - **Alert Severity**
   - **Event Time**
3. You can filter the list of visible alerts by clicking the **Action** drop-down at the top of the table and select **Filter**.
   a. Select the column to filter by from the **Column** drop-down.
   b. Select the an operator from the **Operator** drop-down.
   c. Enter in an appropriate value in the **Expression** field if applicable.
4. Select the check box in the left column to select a specific alert and perform any of the following actions:
   a. Click the **Notify** button, to notify another auditor of the alert. In the **Manual Alert Notification** page, select the template type for the notification. 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.
   b. From the **Set Alert Status** list, select , **Open** or **Closed**to set the alert status, and then click the **Apply** button. When an alert is first generated, it is set to **New**.
   c. Click the **Alert ID** of an alert to get additional details of the alert on the report.

   See Also:

- Creating Custom Alert Status Values
- Logging in to the Audit Vault Server Console

10.5 Creating Custom Alert Status Values

You can create alert status values to assign to an alert during the lifetime of the alert.

Oracle Audit Vault and Database Firewall provides two status values: `New` and `Closed` prior to Oracle AVDF 20.8 and `Open` and `Closed` starting in Oracle AVDF 20.8. You can create additional ones to suit your needs, such as `Pending`.

1. Log in to the Audit Vault Server console as an *auditor*.
2. Click on **Alerts** tab.
3. From the left navigation menu, click on **Manage Alert Status**.

   In this page there are two tabs: **Custom Alert Status** and **Pre-configured Alert Status**. From here you can edit or delete existing alert status values.
4. To create a new alert status, click **Create**.
5. In the **Create Alert Status Value** dialog, 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.
6. Click **Save**.

   The new alert status appears in the **Manage Alert Status** page.

> **See Also:**
>
> - Responding to an Alert to assign alert status.
> - Logging in to the Audit Vault Server Console

10.6 Forwarding Alerts to Syslog

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

As a prerequisite to forwarding alerts to syslog, the Oracle Audit Vault and Database Firewall 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.

1. Log in to the Audit Vault Server console as a super auditor.
2. Click on **Policies** tab.
3. Click on **Alert Policies** tab in the left navigation menu.
4. Click **Forward Alerts to Syslog** button. The button only appears if the Syslog connector is set up by the Oracle AVDF administrator.

   All defined alerts are forwarded to Syslog.

Example 10-1   Oracle Audit Vault and Database Firewall Syslog Alert Message Format

Oracle Audit Vault and Database Firewall alerts appear in syslog in a format similar to the following:

```
[AVDFAlert@111 AN="alert_name" ASE="alert_severity"
URL="auditor_console_URL_for_alert" AT="alert_generated_time"
TN="secured_target" UN="username" AD="alert_description"]
```

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

Example:

```
Apr 16 23:22:31 avs08002707d652 logger: [AVDFAlert@111 AN="w_1" ASE="Warning"
URL=https://192.0.2.10/console/f?p=7700... AT="2014-04-16T22:55:30.462332Z"
TN="cpc_itself" UN="JDOE" AD=" "]
```

See Also:

Logging in to the Audit Vault Server Console

A

Troubleshooting Oracle Audit Vault and Database Firewall for Auditors

Learn how to resolve issues that auditors using Oracle Audit Vault and Database Firewall may encounter.

A.1 Server Error 500 When Logging Into UI as `avauditor`

This error and workaround only applies to Oracle AVDF 20.1-20.4. Starting with Oracle AVDF 20.5 this fix is built into Oracle AVDF.

Issue

The main dashboard page of Oracle AVDF is timing out and causing server error 500 when logging into UI as `avauditor`.

Workaround

Log in to auditor console without accessing the dashboard, by using the following link:

https://<your_ip>/console/f?p=7700:170:840803006486::NO:170::&cs=3sUkbsmjyA0l4dG7esmazo5QHpcHUH-VMcnBdG0LMRQzscQZAV-KmBtzF8wnSPJo3uPv-2avAn3YPBBjzBmOVfA.

Ensure you change <*your_ip*> to the IP address of your Oracle AVDF instance.

A.2 Database Firewall Monitored Activity Report - Error Bad Gateway

Problem

In Oracle AVDF 20.4 and earlier, when you try to fetch the Database Firewall Monitored Activity report for more than 24 hours, you see the following error:

```
Error: Bad Gateway
```

To reproduce the error, log in to the Audit Vault Server console as a super auditor (`AVAUDITOR`). Select the **Reports** tab and navigate to **Activity Reports**, then **Database Firewall Reports**, then **Database Firewall Monitored Activity**. Try to fetch Database Firewall Monitored Activity report for more than 24 hours.

Solution

> **Note:**
>
> This issue was fixed in Oracle AVDF 20.5.

In Oracle AVDF 20.4 and earlier, use the following workaround:

1. Log in to the Audit Vault Server console as an *auditor*.
2. Click the **Reports** tab.
3. Click the **All Activity** report.
4. Add a filter for **Location = 'Network'**.
5. Save the report as "Database Firewall Activity."
6. Click the **Saved Report** tab and open the report that you just saved.

A.3 Is the Audit Vault 20.X EVENT_LOG column RECORD_ID Generated Sequentially or Randomly

It is not guaranteed that the RECORD_ID column will come in sequence. It is guaranteed that RECORD_ID will be unique.

A.4 There is No Option to Filter All Activity Report Using Timestamp/Time

Issue

There is no option to filter the All Activity Report using timestamp/time so that data on a specific day and time can be extracted.

Workaround

Add a row filter in the interactive report. Follow these steps:

1. Log in to the Audit Vault Server Console as an auditor.
2. Click on the **Reports** tab.
3. Click on the **All Activity** report.
4. Select **Filter** from the **Actions** menu.
5. Select the **Row** tab.
6. Enter the following expression:

```
 to_timestamp(to_char(BZ,'MM/DD/YYYY HH:MI:SS PM'),'MM/DD/YYYY HH:MI:SS
PM') >= to_timestamp('11/17/2021 12:35:55 PM','MM/DD/YYYY HH:MI:SS PM')
AND to_timestamp(to_char(BZ,'MM/DD/YYYY HH:MI:SS PM') ,'MM/DD/YYYY
HH:MI:SS PM') <= to_timestamp('11/17/2021 1:05:59 PM' ,'MM/DD/YYYY
HH:MI:SS PM')
```

   Change timestamp in the filter to fit your requirements.

7. Click **Apply**.

A.5 Issue with Data Population in **All Activity by Privileged Users** Report in AVDF 20.4 Installation

Despite successful installation of AVDF 20.4, the **All Activity by Privileged Users** report does not display any data; this is because the Entitlement Job has not yet been executed. This is resolved after executing the job and re-fetching the report.

Symptoms

After a successful AVDF 20.4 installation on a Virtual Machine (VM), with the Agent and Host Monitor successfully installed on the Secured Target, along with Directory and Network trails added, the system is fully operational. All monitoring points are active, and the health indicators of the database firewall are green. The `SYS` user data and Application users data populate in all reports, except the **All Activity by Privileged Users** report.

Cause

The data is not populating in the **All Activity by Privileged Users** report because the Entitlement Job has not been executed for populating the data.

Solution

To resolve this issue, execute the User Entitlement job at least once; see Retrieving User Entitlement Data for Oracle Database Targets for more information. After the successful completion of the job, attempt to fetch the report again. The data should then populate in the **All Activity by Privileged Users** report.

A.6 How to Purge Alert Queue and Alert Store

Issue

If the alerts queue table is long then email notifications for the generated alerts do not send.

Workaround

Perform the following as the `avsys` user.

1. Purge the alert queue table:

```
declare
po dbms_aqadm.aq$_purge_options_t;
begin
po.block := TRUE;
DBMS_AQADM.PURGE_QUEUE_TABLE(
    queue_table=>'avsys.av_alert_qt',
    purge_condition=>NULL,
    purge_options=>po);
END;
```

2. Truncate the tables `alert_store`, `ALERT_TROUBLETICKET_JOB`,`ALERT_EMAIL_JOB`,`ALERT_NOTE`:

   ```
   ALTER TABLE ALERT_TROUBLETICKET_JOB DISABLE CONSTRAINT
   ALRT_TTKT_JOB_ALRT_STORE_FK;
   ALTER TABLE ALERT_EMAIL_JOB DISABLE CONSTRAINT
   ALRT_EMAIL_JOB_ALRT_STORE_FK;
   ALTER TABLE ALERT_NOTE DISABLE CONSTRAINT ALERT_NOTE_ALERT_STORE_FK;

   truncate table alert_store cascade;
   truncate table ALERT_TROUBLETICKET_JOB;
   truncate table ALERT_EMAIL_JOB;
   truncate table ALERT_NOTE;
   ```

3. Reenable the contraints:

   ```
   ALTER TABLE ALERT_NOTE ENABLE CONSTRAINT ALERT_NOTE_ALERT_STORE_FK;
   ALTER TABLE ALERT_TROUBLETICKET_JOB ENABLE CONSTRAINT
   ALRT_TTKT_JOB_ALRT_STORE_FK;
   ALTER TABLE ALERT_EMAIL_JOB ENABLE CONSTRAINT ALRT_EMAIL_JOB_ALRT_STORE_FK;
   ```

A.7 Failed Login Alert Policy

Learn how to configure a failed login alert policy in AVDF using both LOGIN and LOGON command classes.

Issue

The Failed Login alert policy is enabled, but the alert condition does not trigger properly. The current condition is:

```
:COMMAND_CLASS = 'LOGON'
AND
:EVENT_STATUS = 'FAILURE'
```

The policy does not capture all failed login attempts as expected.

Workaround

To resolve this issue, update the alert condition to include both `LOGIN` and `LOGON` command classes to ensure all failed login attempts are captured. Additionally, to filter alerts by target, include the `:SECURED_TARGET_NAME IN()` clause.

Revised condition:

```
: COMMAND_CLASS ='LOGON','LOGIN'
AND
:EVENT_STATUS ='FAILURE'
Group By -:SECURED_TARGET_NAME IN()
```

This revised condition ensures comprehensive alerting for all failed login events across the specified secured targets.

B

Oracle Audit Vault and Database Firewall Database Schemas

Learn about the Oracle Audit Vault and Database Firewall schemas.

B.1 About Oracle Audit Vault and Database Firewall Schemas

Oracle Audit Vault and Database Firewall has internal data warehouse schemas that manage the audit data collected from the targets.

The data warehouse schemas collect the data from the Oracle Audit Vault and Database Firewall collection agents, organize it, and then provide it in report format.

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 targets—Oracle Database, Microsoft SQL Server, Sybase Adaptive Server Enterprise (ASE), and IBM DB2.

You can create these kinds of custom reports:

- Activity reports
- Event reports
- Alert reports
- Entitlement reports

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

> **See Also:**
>
> - Reports
> - Audit Record Fields
> - IBM DB2 Audit Events

B.2 Metadata for Activity Reports

The metadata for activity reports captures data such as connect strings and creation times.

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

- Table B-1

- Table B-2
- Table B-3

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

Table B-1 AVSYS.SECURED_TARGET Table

Column	Data Type	Description
ACTIVE	CHAR(1 CHAR)	'Y' if target is active, 'N' otherwise.
CONNECT_STRING	VARCHAR2(4000 BYTE)	String that identifies target when you try to connect it to the system.
CREATION_TIME	TIMESTAMP WITH LOCAL TIME ZONE	Creation time of the connection between target and the system.
DESCRIPTION	VARCHAR2(1024 BYTE)	Description of target.
FIREWALL_POLICY_ID	INTEGER	ID number of firewall policy associated with target, if any; otherwise NULL. Default: NULL
SECURED_TARGET_ID	NUMBER	ID of the target.
SECURED_TARGET_NAME	VARCHAR2(255 BYTE)	Name of target.
SECURED_TARGET_TYPE_ID	NUMBER	ID number of type of target. This value must be in AVSYS.SECURED_TARGET_TYPE.SECURED_TARGET_TYPE_ID (see Table B-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 B-2 describes the AVSYS.SECURED_TARGET_TYPE table, which has one row for each target type. Columns are in alphabetical order.

Table B-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 target type.
SECURED_TARGET_TYPE_NAME	VARCHAR2(255 BYTE)	Name of target type.

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

Table B-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).

Table B-3 (Cont.) AVSYS.AUDIT_TRAIL Table

Column	Data Type	Description
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 target for this audit trail. This value must be in AVSYS.SECURED_TARGET_TYPE.SECURED_TARGET_TYPE_NAME (see Table B-2).

B.3 Data for Event Reports

The metadata for event reports captures data such as actions taken or alerts raised.

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

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

Table B-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_ID	VARCHAR2(1024 CHAR)	Client identifier of the user whose actions were audited
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.

Table B-4 (Cont.) AVSYS.EVENT_LOG Table

Column	Data Type	Description
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).
DATA_TRACE	CLOB	Transaction log data (before and after values) in JSON format.
ERROR_CODE	VARCHAR2(30 BYTE)	Error code of an action.
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, Database Object, 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.

Table B-4 (Cont.) AVSYS.EVENT_LOG Table

Column	Data Type	Description
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.
POLICY_NAME Oracle AVDF 20.3 and later	VARCHAR2(4000 CHAR)	Name of policy file that the Database Firewall used when it detected the event. In case of audit data collected by the Agent, the policy name contains the audit policies that caused the current event.
RECORD_ID	NUMBER	ID number of audit record for the event.
SECURED_TARGET_NAME	VARCHAR2(255 BYTE)	Name of target where event occurred.
SECURED_TARGET_TYPE	VARCHAR2(255 BYTE)	Type of 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.
TERMINAL	VARCHAR2(255 CHAR)	Name of the terminal (for example, Unix terminal) that was the source of the event

Table B-4 (Cont.) AVSYS.EVENT_LOG Table

Column	Data Type	Description
THREAT_SEVERITY	VARCHAR2(30 CHAR)	The severity of the threat detected by the Database Firewall. This field may have one of the values: minimal, minor, moderate, major, or critical. The threat severity differentiates the importance of each event. This is defined in the Database Firewall policy. You can choose the value for each rule that triggers the event. The Database Firewall policy auditor can apply their own judgement when choosing the value assigned to each rule. This severity level later appears in the reports if the statement is logged. **Note:** In Oracle AVDF release 20.5 and prior, the pre-defined Database Firewall policy does not define the threat severity value. In the reports it would appear as undefined.
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.
AUDIT_TYPE Oracle AVDF 20.3 and later	VARCHAR2(255 CHAR)	Audit types for Oracle Database target: • Standard • FineGrainedAudit • XS • Database Vault • Label Security • RMAN_AUDIT • Datapump • Direct path API
APPLICATION_CONTEXT Oracle AVDF 20.3 and later	VARCHAR2(4000 BYTE)	Application context information.
DATABASE_NAME Oracle AVDF 20.4 and later	VARCHAR2(255 CHAR)	The name of the DB2 database that contains the audit records.
INSTANCE_NAME Oracle AVDF 20.4 and later	VARCHAR2(255 CHAR)	The name of the instance which hosts the DB2 database.
AUDIT_TRAIL_ID	NUMBER	The ID of the audit trail.
LOCATION	VARCHAR2(30 CHAR)	The location of the audit trail. For example: Audit Table or Audit File.
REPOSITORY_NAME	VARCHAR2(255 CHAR)	PDB name of the CDB target.

Table B-4 (Cont.) AVSYS.EVENT_LOG Table

Column	Data Type	Description
ROW_COUNT	NUMBER	Number of rows returned (Database Firewall).
SECURED_TARGET_CLASS	VARCHAR2(30 CHAR)	The type of the target. For example: database or operating system.
SECURED_TARGET_ID	NUMBER NOT NULL	ID of the target.

B.4 Data for Alert Reports

The metadata for alert reports captures data such as alert definitions and alert IDs.

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

- Table B-5
- Table B-6
- Table B-7

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

Table B-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.
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.

Table B-5 (Cont.) AVSYS.ALERT_STORE Table

Column	Data Type	Description
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 B-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 B-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 the event related to this alert instance.
SECURED_TARGET_ID	NUMBER NOT NULL	The ID of the target.
SECURED_TARGET_NAME	VARCHAR2(255 CHAR) NOT NULL	The name of the target.
USER_NAME	VARCHAR2(255 CHAR)	The user name of the event.

Table B-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 B-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	CONTAINER VARCHAR2(30)	Content of this note.
NOTE_CREATOR	VARCHAR2(30)	User who created this note.
NOTE_OWNER	VARCHAR2(30)	Owner of this note, same as alert definition.

Table B-7 (Cont.) AVSYS.ALERT_NOTE Table

Column	Data Type	Description
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.

B.5 Data for Entitlement Reports

The metadata for entitlement reports captures data such as package, role, and schema entitlements.

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

- Table B-8
- Table B-9
- Table B-10
- Table B-11
- Table B-12
- Table B-13
- Table B-14
- Table B-15
- Table B-16
- Table B-17
- Table B-18

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

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

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

Table B-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

Table B-15 (Cont.) AVSYS.UE_DBA_USERS

Column	Data Type	Description
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
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 B-16 describes the AVSYS.UE_ROLE_SYS_PRIVS table, which stores information about system privileges granted to roles. Columns are in alphabetical order.

Table B-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 B-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 B-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

Table B-17 (Cont.) AVSYS.UE_ROLE_TAB_PRIVS

Column	Data Type	Description
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 B-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 B-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

B.6 Data for SPA Reports

The metadata for stored Stored Procedure Auditing (SPA) reports captures data such as target IDs and object IDs.

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

- Table B-19
- Table B-20

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

Table B-19 AVSYS.SPA_OBJECTS

Column	Data Type	Description
ID	INTEGER	Unique identifier for the object
SECURED_TARGET_ID	INTEGER	The 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)	Comma-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
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 B-20 describes the AVSYS.SPA_EDITS table, which stores data about, and the content of, stored procedure edits.

Table B-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 (255 CHAR)	The database user that modified the object
CHANGED_AT	TIMESTAMP WITH LOCAL TIME ZONE	The date and time when the object was changed

Table B-20 (Cont.) AVSYS.SPA_EDITS

Column	Data Type	Description
DETECTED_AT	TIMESTAMP WITH LOCAL TIME ZONE	The date and time when the change was detected on the controller

B.7 Data for Database Firewall Reports

The metadata for custom Database Firewall reports captures data such as target databases and types of statements included.

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

- Table B-21
- Table B-22

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

Table B-21 AVSYS.FW_CLUSTER

Column	Data Type	Description
ID	NUMBER	Cluster global identifier
SECURED_TARGET_ID	INTEGER	The target database for this cluster
GRAMMAR_VERSION	INTEGER	Version number of the Database Firewall grammar
FIREWALL_DIALECT	SMALLINTEGER	Database type of the cluster. **See Also:** Table B-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 B-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 B-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

Table B-22 (Cont.) AVSYS.FW_CLUSTER_COMPONENT

Column	Data Type	Description
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'

C Data Warehouse Partition

You should understand the data warehousing and partition functionality of the Audit Vault and Database Firewall system.

The Audit Vault and Database Firewall data warehouse uses partition functionality. The data warehouse creates partitions and sub partitions in the `event_log` and `event_log_arch` tables.

The following are the highlights of partition functionality in release 12.2.0.4.0 and older:

- Partition is created daily by default.
- The daily partition has a default sub partition with a *high_value* as *null*.
- The partition naming convention is `DWFACT_P<Year YYYY><Month MM><Day DD>`.
- Every partition has a subpartition for each target that collects for the date of partition. The *high_value* of subpartition is the target ID.

Monthly Data Warehouse Partition

The monthly partition is applicable from release 12.2.0.5.0 and onwards. The older releases have the daily partition.

The following are the highlights of the monthly partition that creates partitions and sub partitions in the `event_log` and `event_log_arch` tables.

- A month can either have the monthly or the daily partition. In case a specific month already has a partition for a specific day, then the data continues to have the daily partition.
- In case of a new installation, the system has monthly partition only.
- In case of upgraded system, both daily and monthly partitions exist. In such systems where there are daily partitions already existing, those partitions continue to have the daily partition. The remaining days in that month when the upgrade is performed will also continue to have the daily partition. Any month which does not have any pre existing daily partition will have monthly partition.
- The previously created partition have both the partitions as described above depending on the system.
- The naming convention for a daily partition is `DWFACT_P<Year YYYY><Month MM><Day DD>`.
- The naming convention for a monthly partition is `DWFACT_P<yyyy><MM><01>`, which is executed on the first day of every month.
- The monthly and daily partition have a sub partition for every target with one default sub partition.

Partition Functionality Matrix

Partition Type	Naming Convention	Log Tables	Sub Partition
Daily Partition	`DWFACT_P<Year YYYY><Month MM><Day DD>`	`event_log` `event_log_arch`	• One default subpartition created where the *high value* is *null*. • One subpartition created for which the data has been collected for a specific date, where the *high value* is equal to the Target ID.
Monthly Partition	`DWFACT_P<yyyy><MM><01>`	`event_log` `event_log_arch`	• One default subpartition created where the *high value* is *null*. • One subpartition created for which the data has been collected for a specific month, where the *high value* is equal to the Target ID.

Oracle Database In-Memory

The data can be saved in Oracle Database In-Memory. To achieve this Oracle Database In-Memory has to be enabled.

> **Note:**
>
> See Enabling Oracle Database In-Memory for the Audit Vault Server for more information.

Starting release 12.2.0.5.0 onwards, a minimum of one month data is stored in Oracle Database In-Memory. In case date range is not selected then the data is saved in Oracle Database In-Memory starting from the recent month to the oldest, depending on the available memory size. In case of date range selection, data is saved in Oracle Database In-Memory starting from the recent month to the oldest month of the selected period depending on the available memory size.

Prior to release 12.2.0.5.0, a minimum of one day data is stored in Oracle Database In-Memory. In case date range is not selected then the data is saved in Oracle Database In-Memory starting from the recent day to the oldest, depending on the available memory size. In case of date range selection, data is saved in Oracle Database In-Memory starting from the recent day to the oldest day of the selected period depending on the available memory size.

D
Audit Record Fields

Audit record fields capture data such as target, service, and policy names.

Table D-1 lists the fields in an Oracle AVDF audit record.

Table D-1   Audit Record Fields

Audit Record Field	Description	Column Type
Target Name	Target system secured by AVDF	`VARCHAR(255)`
Target Type	Type of target, for example, Microsoft SQL Server, IBM DB2 etc.	`VARCHAR2(255)`
Service Name	Target service used to perform this event	`VARCHAR2 (255 CHAR)`
Policy Name	Name of the policy when the event was recorded	`VARCHAR2(1024)`
Policy Name From Oracle AVDF 20.3 and later	Name of the policy which caused the event	`VARCHAR2(4000 CHAR)`
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	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 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
Object	Object affected by event	`VARCHAR2(255)`
Object Type	Type of target object, for example, Package, Type, Table	`VARCHAR2(255)`
Object Owner	Owner of target object	`VARCHAR2(255)`
Terminal	Name of the terminal (for example, Unix terminal) that was the source of the event	`VARCHAR2(255 CHAR)`
OS User Name	Operating system login name of the target user causing the event	`VARCHAR2(255)`
Client Host Name	Name of the host machine	`VARCHAR2(255)`
Client ID	Client identifier of the user whose actions were audited	`VARCHAR2(1024 CHAR)`
Client IP	IP address of the Client Host	`VARCHAR2(255)`

Table D-1   (Cont.) Audit Record Fields

Audit Record Field	Description	Column Type
Network Connection	Description of the network connection	`VARCHAR2(255)`
Client Program	Name of program on Client Host that issued command	`VARCHAR2(255)`
Command Text	Command statement issued by target user	`CLOB` Securefile
Command Param	Parameters associated with command text	`CLOB`
Extension	Additional detailed information about the audited event	`CLOB` Securefile
Original Content	Audit record generated by target	`CLOB` Securefile
Command Class	Class of command issued by target user that caused the event	`VARCHAR2(255)`
Audit Type	Type of auditing (Oracle AVDF 20.3 and later)	`VARCHAR2(255 CHAR)`
Application Context	Application context information (Oracle AVDF 20.3 and later)	`VARCHAR2(4000 BYTE)`

E
Oracle Database Audit Events

Audit events are in a wide variety of categories, such as account management events and peer association events.

E.1 About the Oracle Database Audit Events

The audit events are categorized into events such as account management or audit command 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 Audit Vault and Database Firewall 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.

Note:

Oracle AVDF's support of Oracle Database 11g is deprecated in AVDF 20.14, and will be desupported in AVDF 20.15.

See Also:

Oracle Audit Vault and Database Firewall Database Schemas for Oracle Audit Vault and Database Firewall data warehouse details that may be useful in designing your own reports.

E.2 Account Management Events

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

Table E-1 lists the Oracle Database account management audit events and the equivalent Oracle AVDF events.

Table E-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

Table E-1 (Cont.) Oracle Database Account Management Audit Events

Source Event	Event Description	Command Class	Target Type
DROP PROFILE	Drop Profile	DROP	PROFILE
DROP USER	Drop User	DROP	USER

E.3 Application Management Events

Application management events track actions that were performed on the underlying PL/SQL procedures or functions of system services and applications.

An example of such statements are ALTER FUNCTION statements.

Table E-2 lists the Oracle Database application management audit events and the equivalent Oracle AVDF events.

Oracle AVDF's support of Oracle Database 11g is deprecated in AVDF 20.14, and will be desupported in AVDF 20.15.

Table E-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

Table E-2 (Cont.) Oracle Database Application Management Audit Events

Source Event	Event Description	Command Class	Target Type
CREATE JAVA	Create Java	CREATE	JAVA
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

E.4 Audit Command Events

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

Table E-3 lists the Oracle Database audit command audit events and the equivalent Oracle AVDF events.

Table E-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

E.5 Data Access Events

Data access events track audited data manipulation language (DML) activities.

Examples of such activies are all SELECT, INSERT, UPDATE, or DROP SQL statements. The Data Access Report uses these events.

Table E-4 lists the Oracle Database data access audit events and the equivalent Oracle Audit Vault and Database Firewall events.

Table E-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) Oracle AVDF's support of Oracle Database 11g is deprecated in AVDF 20.14, and will be desupported in AVDF 20.15.	SELECT	MINING MODEL
TRUNCATE TABLE	Truncate Table	TRUNCATE	TRUNCATE TABLE
UPDATE	Update	UPDATE	NULL

See Also:

Data Access Report

E.6 Database Vault Events

Oracle Database Vault tracked events cover Database Vault releases 11g and 12c.

E.6.1 Database Vault Events in Oracle Database 11g

Tracked Oracle Database Vault events from release 11g include Database Vault APIs that manage factors, rules, and other Database Vault components.

Oracle AVDF's support of Oracle Database 11g is deprecated in AVDF 20.14, and will be desupported in AVDF 20.15.

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

Table E-5 Database Vault Audit Events in Oracle Database 11*g*

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

E.6.2 Database Vault Events in Oracle Database 12c

Tracked Oracle Database Vault events from release 12c include Database Vault APIs that manage factors, rules, and other Database Vault components.

Table E-6 lists Database Vault events for Oracle Database 12c databases that have Database Vault enabled.

Table E-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
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

Table E-6 (Cont.) Database Vault Audit Events in Oracle Database 12c

Source Event	Event Description	Command Class	Target Type
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
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

Table E-6 (Cont.) Database Vault Audit Events in Oracle Database 12c

Source Event	Event Description	Command Class	Target 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
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

Table E-6 (Cont.) Database Vault Audit Events in Oracle Database 12c

Source Event	Event Description	Command Class	Target Type
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

E.7 Exception Events

Exception events track audited error and exception activity, such as network errors.

Table E-7 lists the Oracle Database exception audit events and the equivalent Oracle Audit Vault and Database Firewall event.

Table E-7 Oracle Database Exception Audit Event

Source Event	Event Description	Command Class	Target Type
ERROR NETWORK	Network Error	ERROR	NETWORK

E.8 Invalid Record Events

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

Table E-8 lists the Oracle Database invalid record audit events and the equivalent Oracle AVDF event.

Table E-8 Oracle Database Invalid Record Audit Event

Source Event	Event Description	Command Class	Target Type
INVALID RECORD	Invalid Record	INVALID	RECORD

E.9 Object Management Events

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

Table E-9 lists the Oracle Database object management audit events and the equivalent Oracle AVDF events.

Oracle AVDF's support of Oracle Database 11g is deprecated in AVDF 20.14, and will be desupported in AVDF 20.15.

Table E-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

Table E-9 (Cont.) Oracle Database Object Management Audit Events

Source Event	Event Description	Command Class	Target Type
CREATE DIRECTORY	Create Directory	CREATE	DIRECTORY
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

Table E-9 (Cont.) Oracle Database Object Management Audit Events

Source Event	Event Description	Command Class	Target Type
DROP TABLE	Drop Table	DROP	TABLE
DROP VIEW	Drop View	DROP	VIEW
FLASHBACK TABLE	Flashback Table	RETRIEVE	TABLE
LOCK	Lock	LOCK	NULL
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.

E.10 Peer Association Events

Peer association events track database link statements.

Table E-10 lists the Oracle Database peer association audit events and the equivalent Oracle AVDF events.

Table E-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

E.11 Role and Privilege Management Events

Role and privilege management events track audited role and privilege management activity, such as granting object permissions to a user.

Table E-11 lists the Oracle Database role and privilege management audit events and the equivalent Oracle AVDF events.

Table E-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
SET USER PROGRAM UNIT LABEL	Set User or Program Unit Label[1]	SET PROGRAM	USER 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.

E.12 Service and Application Utilization Events

Service and application utilization events track audited application access activity, such as the execution of PL/SQL procedures or functions.

Table E-12 lists the Oracle Database service and application utilization audit events and the equivalent Oracle Audit Vault and Database Firewall events.

Table E-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

E.13 System Management Events

System management events track audited system management activity, such as STARTUP and SHUTDOWN operations.

Table E-13 lists the Oracle Database system management audit events and the equivalent Oracle Audit Vault and Database Firewall events.

Oracle AVDF's support of Oracle Database 11g is deprecated in AVDF 20.14, and will be desupported in AVDF 20.15.

Table E-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
CREATE CONTROL FILE	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

Table E-13 (Cont.) Oracle Database System Management Audit Events

Source Event	Event Description	Command Class	Target Type
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

E.14 Unknown or Uncategorized Events

Unknown or uncategorized events track audited activity that cannot be categorized, such as ALTER SUMMARY statements.

Table E-14 lists the Oracle Database unknown or uncategorized audit events and the equivalent Oracle Audit Vault and Database Firewall events.

Table E-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

E.15 User Session Events

User session events track audited authentication events for users who log in to the database.

Table E-15 lists the Oracle Database user session audit events and the equivalent Oracle Audit Vault and Database Firewall events.

Table E-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
SESSION REC	Session Record	MERGE	SESSION RECORD
SET ROLE	Set Role	SET	ROLE
SET TRANSACTION	Set Transaction	SET	TRANSACTION
SUPER USER LOGON	Super User Logon	LOGON	SUPER USER

F

AIX Audit Events

AIX audit events include AIX-related commands, such as PROC_Create.

The following table lists the AIX Audit Events.

Table F-1 AIX Audit Events

Source Event	Event Description	Command Class	Target Type
PROC_Create	Creates a new process.	CREATE	PROCEDURE
PROC_Delete	Terminates the calling process.	DELETE	PROCEDURE
PROC_Execute	Executes a new program.	EXECUTE	PROCEDURE
FILE_Accessx	Determines the accessibility of a file	RETRIEVE	FILE
FILE_StatAcl	Retrieves the access control information for a file.	RETRIEVE	FILE
FILE_Frevoke	Revokes access to a file by other processes.	REVOKE	FILE
PROC_Environ	Change various piece of user information data.	ALTER	USER_INFORMATION
PROC_SetSignal	Action to take upon delivery of signal.	SET	PROCEDURE
PROC_Limits	Controls max system resource consumption	SET	SYSTEM_RESOURCE
PROC_Setpri	Sets fixed priority for process.	EXECUTE	FUNCTION
PROC_Privilege	Changes one or more privilege vectors for process.	ALTER	PROCESS
PROC_Settimer	Sets current value for a specified system wide timer.	SET	TIMER
PROC_Adjtime	Changes system clock.	ALTER	SYSTEM_CLOCK
PROC_Debug	Traces the execution of another process.	TRACE	PROCESS
PROC_Kill	Sends a signal to a process or group of processes.	STOP	PROCESS
PROC_setpgid	Sets the process id group.	SET	PROCESS_ID
PROC_Load	Loads new object module into process address space.	ASSIGN	PROCESS
PROC_SetGroups	Change process concurrent group set.	ALTER	PROCESS
PROC_Sysconfig	Calls to the sysconfig subroutine.	EXECUTE	SYSCONFIG
AUD_Bin_Def	Modification of auditbin.	ALTER	AUDIT_BIN
AUD_Events	Modification of Events.	ALTER	AUDIT_EVENTS
AUD_Objects	Modification of auditobj.	ALTER	AUDIT_OBJETCS
ACCT_Disable	Disables system accounting.	DISABLE	SYSTEM_ACCOUNTING
ACCT_Enable	Enables system accounting.	ENABLE	SYSTEM_ACCOUNTING

Table F-1 (Cont.) AIX Audit Events

Source Event	Event Description	Command Class	Target Type
FILE_Open	calls to the open subroutine.	OPEN	FILE
FILE_Read	Reads from file descriptor.	READ	FILE
FILE_Write	Writes data to descriptor.	WRITE	FILE
FILE_Close	Closes open file descriptor.	CLOSE	FILE
FILE_Link	Creates new directory entry for file.	CREATE	LINK
FILE_Unlink	Removes a file system object.	DELETE	FILE
FILE_Rename	Changes name of a file system object.	RENAME	FILE
FILE_Owner	Changes file ownership.	ALTER	OWNER
FILE_Mode	Changes file mode.	ALTER	FILE
FILE_Fchmod	Changes file permission for file descriptor	ALTER	FILE
FILE_Fchown	Changes ownership for file descriptor.	ALTER	FILE
FILE_Truncate	Calls to the truncate subroutine.	TRUNCATE	FILE
FILE_Symlink	Creates symbolic link.	CREATE	SYMBOLIC_LINK
FILE_Pipe	Creates unnamed pipe.	CREATE	PIPE
FILE_Mknod	Calls to the mknod subroutine.	CREATE	NODE
FILE_Dupfd	Duplicates file descriptor.	COPY	FILE
FS_Extend	Extends file system.	EXTEND	FILE
FS_Mount	Connects file system to named directory.	CONNECT	FILE
FS_Umount	Disconnects mounted file system.	DISCONNECT	FILE
FILE_Acl	Changes file access control list (ACL)	ALTER	FILE
FILE_Facl	Changes ACL for file descriptor.	ALTER	FILE_DESCRIPTOR
FILE_Privilege	Calls to the chpriv subroutine.	ALTER	PRIVILEGE
FILE_Chpriv	Changes privilege control list.	ALTER	PRIVILEGE_CONTROL_LIST
FILE_Fchpriv	Changes PCL for file descriptor.	ALTER	FILE_DESCRIPTOR
FS_Chdir	Changes current working directory.	ALTER	DIRECTORY
FS_Fchdir	Changes current working directory by file descriptor.	ALTER	DIRECTORY
FS_Chroot	Changes meaning of “/” for current process.	ALTER	PROCESS
FS_Rmdir	Removes directory object.	DELETE	DIRECTORY
FS_Mkdir	Creates directory.	CREATE	DIRECTORY
FILE_Utimes	Calls to the utimes subroutine.	EXECUTE	PROCESS
FILE_Stat	Calls to the stat subroutine.	EXECUTE	PROCESS
MSG_Create	Creates new message queue.	CREATE	QUEUE
MSG_Read	Receives message from message queue.	RECEIVE	MESSAGE
MSG_Write	Sends message on message queue.	SEND	MESSAGE

Table F-1 (Cont.) AIX Audit Events

Source Event	Event Description	Command Class	Target Type
MSG_Delete	Removes message queue.	DELETE	MESSAGE
MSG_Owner	Changes ownership and access right of message queue.	ALTER	MESSAGE_QUEUE
MSG_Mode	Queries semaphore set access rights.	SET	ACCESS_RIGHTS
SHM_Create	Creates new shared memory segment.	CREATE	MEMORY_SEGMENT
SHM_Open	Calls to the shmat subroutine with Open option.	OPEN	MEMORY_SEGMENT
SHM_Detach	Calls to the shmat subroutine with Detach option.	DISASSOCIATE	MEMORY_SEGMENT
SHM_Close	Closes shared memory segment.	CLOSE	MEMORY_SEGMENT
SHM_Owner	Changes ownership and access rights for shared memory segment.	ALTER	MEMORY_SEGMENT
SHM_Mode	Queries access rights of shared memory segment.	ACCESS	MEMORY_SEGMENT
TCPIP_config	Logs changes to TCP/IP interface.	WRITE	TCP/IP
TCPIP_host_id	Logs attempts to change system host name.	WRITE	TCP/IP
TCPIP_route	Logs changes to routing table.	WRITE	TCP/IP
TCPIP_connect	Calls to the connect subroutine.	CONNECT	TCP/IP
TCPIP_data_out	Data sent.	SEND	TCP/IP
TCPIP_data_in	Data received.	RECEIVE	TCP/IP
TCPIP_set_time	Logs attempt to change system time via network.	SET	TCP/IP
TCP_ksocket	Calls to the kernel TCPIP kernel services.	EXECUTE	TCP/IP
TCP_ksocketpair	Calls to the kernel TCPIP kernel services.	EXECUTE	TCP/IP
TCP_kclose	Calls to the kernel TCPIP kernel services.	CLOSE	TCP/IP
TCP_ksetopt	Calls to the kernel TCPIP kernel services.	SET	TCP/IP
TCP_kbind	Calls to the kernel TCPIP kernel services.	CONNECT	TCP/IP
TCP_klisten	Calls to the kernel TCPIP kernel services.	COMMUNICATE	TCP/IP
TCP_kconnect	Calls to the kernel TCPIP kernel services.	CONNECT	TCP/IP
TCP_kaccept	Calls to the kernel TCPIP kernel services.	CONNECT	TCP/IP
TCP_kshutdown	Calls to the kernel TCPIP kernel services.	SHUTDOWN	TCP/IP
TCP_ksend	Calls to the kernel TCPIP kernel services.	SEND	TCP/IP

Table F-1 (Cont.) AIX Audit Events

Source Event	Event Description	Command Class	Target Type
TCP_kreceive	Calls to the kernel TCPIP kernel services.	RECEIVE	TCP/IP
USER_Login	Calls to the Terminal State Management service.	LOGIN	ACCOUNT
SYSCK_Check	Calls to the sysck function.	EXECUTE	PROCEDURE
SYSCK_Update	Calls to the sysck function.	UPDATE	PROCEDURE
SYSCK_Install	Calls to the sysck function.	INSTALL	PROCEDURE
SYSCK_Delete	Calls to the sysck function.	DELETE	PROCEDURE
TCBCK_Check	Calls to the tcbck function.	EXECUTE	FUNCTION
TCBCK_Update	Calls to the tcbck function.	UPDATE	FUNCTION
TCBCK_Delete	Calls to the tcbck function.	DELETE	FUNCTION
USER_Check	Calls to the usrck function. USRCK_Error	EXECUTE	FUNCTION
USER_Logout	Calls to the logout subroutine.	LOGOUT	USER
PORT_Change	Calls to the chsec subroutine.	ALTER	PORT
USER_Change	Calls to the chuser subroutine.	ALTER	USER
USER_Remove	Removes a user.	DELETE	USER
USER_Create	Creates a user.	CREATE	USER
USER_SetGroups	Calls to the setgroups subroutine.	SET	GROUP
USER_SetEnv	Calls to the setenv subroutine.	SET	USER
USER_SU	Calls to the su subroutine.	LOGIN	USER
GROUP_User	Calls to the grpchk subroutine.	EXECUTE	PROCEDURE
GROUP_Adms	Calls to the grpchk subroutine.	EXECUTE	PROCEDURE
GROUP_Change	Calls to the chgroup subroutine.	ALTER	GROUP
GROUP_Create	Calls to the mkgroup subroutine.	CREATE	GROUP
GROUP_Remove	Calls to the rmgroup subroutine.	DELETE	GROUP
PASSWORD_Change	Changes a user password.	UPDATE	USER
PASSWORD_Flags	Calls to the pwdadm subroutine.	ALTER	USER
PASSWORD_Check	Calls to the pwdck subroutine.	ALTER	USER
SRC_Start	Starts a system resource controller.	START	CONTROLLER
SRC_Stop	Stops a system resource controller.	STOP	CONTROLLER
SRC_Addssys	Calls to the addsys subroutine.	EXECUTE	PROCEDURE
SRC_Chssys	Calls to the chssys subroutine.	EXECUTE	PROCEDURE
SRC_Addserver	Calls to the addserver subroutine.	EXECUTE	PROCEDURE
SRC_Chserver	Calls to the chserver subroutine.	EXECUTE	PROCEDURE
SRC_Delssys	Calls to the rmsys subroutine.	EXECUTE	PROCEDURE
SRC_Delserver	Calls to the rmserver subroutine.	EXECUTE	PROCEDURE
ENQUE_admin	Calls to the enq subroutine.	EXECUTE	PROCEDURE

Table F-1 (Cont.) AIX Audit Events

Source Event	Event Description	Command Class	Target Type
ENQUE_exec	Calls to the qdaemon subroutine.	EXECUTE	PROCEDURE
SENDMAIL_Config	Calls to the sendmail function.	EXECUTE	FUNCTION
SENDMAIL_ToFile	Calls to the sendmail function.	EXECUTE	FUNCTION
AT_JobAdd	Calls to the at function.	EXECUTE	FUNCTION
At_JobRemove	Calls to the at function.	EXECUTE	FUNCTION
CRON_JobRemove	Calls to the cron function.	EXECUTE	FUNCTION
CRON_JobAdd	Start of a cron job.	START	CRON
CRON_Start	End of a cron job.	START	SYSTEM
NVRAM_Config	Access to the NVRAM.	ACCESS	NVRAM
DEV_Configure	Calls to the cfgmgr function.	CONFIGURE	FUNCTION
DEV_Change	Device changed.	ALTER	DEVICE
DEV_Create	Device created.	CREATE	DEVICE
DEV_Start	Device started.	START	DEVICE
INSTALLP_Inst	Calls to the installp function.	EXECUTE	FUNCTION
INSTALLP_Exec	Calls to the installp function.	EXECUTE	FUNCTION
DEV_Stop	Device stopped.	STOP	DEVICE
DEV_Unconfigure	Device unconfigured.	DISASSOCIATE	DEVICE
DEV_Remove	Device removed.	DELETE	DEVICE
DSMIT_start	Calls to the dsmit function.	EXECUTE	FUNCTION
DSMIT_end	Calls to the dsmit function.	EXECUTE	FUNCTION
LVM_ChangeLV	Calls to the lvm function.	EXECUTE	FUNCTION
LVM_ChangeLV	Calls to the lvm function.	EXECUTE	FUNCTION
LVM_ChangeLV	Calls to the lvm function.	EXECUTE	FUNCTION
LVM_ChangeVG	Calls to the lvm function.	EXECUTE	FUNCTION
LVM_ChangeVG	Calls to the lvm function.	EXECUTE	FUNCTION
LVM_ChangeVG	Calls to the lvm function.	EXECUTE	FUNCTION
LVM_CreateLV	Calls to the lvm function.	EXECUTE	FUNCTION
LVM_CreateVG	Calls to the lvm function.	EXECUTE	FUNCTION
LVM_DeleteVG	Calls to the lvm function.	EXECUTE	FUNCTION
LVM_DeleteLV	Calls to the lvm function.	EXECUTE	FUNCTION
LVM_VaryoffVG	Calls to the lvm function.	EXECUTE	FUNCTION
LVM_VaryonVG	Calls to the lvm function.	EXECUTE	LVM
LVM_AddLV	Calls to the lvm function.	ADD	LVM
LVM_KDeleteLV	Calls to the lvm function.	DELETE	LVM
LVM_KDeleteVG	Deletes a volume group from the kernel.	DELETE	VOLUME_GROUP
LVM_ExtendLV	Calls to the lvm function.	UPDATE	LVM
LVM_ReduceLV	Calls to the lvm function.	UPDATE	LVM
LVM_KChangeLV	Calls to the lvm function.	UPDATE	LVM
LVM_AvoidLV	Calls to the lvm function.	UPDATE	LVM

Table F-1 (Cont.) AIX Audit Events

Source Event	Event Description	Command Class	Target Type
LVM_MissingPV	Calls to the lvm function.	UPDATE	PHYSICAL_VOLUME
LVM_AddPV	Calls to the lvm function.	ADD	PHYSICAL_VOLUME
LVM_AddMissPV	Calls to the lvm function.	ADD	PHYSICAL_VOLUME
LVM_DeletePV	Calls to the lvm function.	DELETE	PHYSICAL_VOLUME
LVM_RemovePV	Calls to the lvm function.	DROP	PHYSICAL_VOLUME
LVM_AddVGSA	Calls to the lvm function.	ADD	PHYSICAL_VOLUME
LVM_DeleteVGSA	Calls to the lvm function.	DELETE	PHYSICAL_VOLUME
LVM_SetupVG	Calls to the lvm function.	SET	VOLUME_GROUP
LVM_DefineVG	Calls to the lvm function.	CREATE	VOLUME_GROUP
LVM_ChgQuorum	Calls to the lvm function.	UPDATE	VOLUME_GROUP
LVM_Chg1016	Calls to the lvm function.	UPDATE	VOLUME_GROUP
LVM_UnlockDisk	Calls to the lvm function.	UNLOCK	VOLUME_GROUP
LVM_LockDisk	Calls to the lvm function.	LOCK	VOLUME_GROUP
BACKUP_Export	Calls to the backup/restore function.	BACKUP	SYSTEM
BACKUP_Priv	Calls to the backup/restore function.	BACKUP	PRIVILEGE
RESTORE_Import	Calls to the backup/restore function.	RESTORE	SYSTEM
USER_Shell	Access to the shell.	ACCESS	SHELL
USER_Reboot	Calls to the reboot function.	START	SYSTEM
PROC_Reboot	Calls to the reboot function.	START	SYSTEM

G

Sybase ASE Audit Events

Sybase ASE audit events cover categories such as account management events and application management events.

G.1 About the Sybase ASE Audit Events

The Sybase ASE audit events include categories such as account management events and application management 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 Audit Vault and Database Firewall 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 for Oracle Audit Vault and Database Firewall data warehouse details that may be useful in designing your own reports.

G.2 Account Management Events

Account management events track Transact-SQL commands that affect user accounts, such as the `UNLOCK ADMIN ACCOUNT` command.

Table G-1 lists the Sybase ASE account management events and the equivalent Oracle AVDF events.

Table G-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`

G.3 Application Management Events

Application management events track actions performed on the underlying Transact-SQL commands of system services and applications, such as the `CREATE RULE` command.

Table G-2 lists the Sybase ASE application management events and the equivalent Oracle AVDF events.

Table G-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

G.4 Audit Command Events

Audit command events track the use of auditing Transact-SQL commands on other Transact-SQL commands and on database objects.

Table G-3 lists the Sybase ASE audit command events and the equivalent Oracle AVDF events.

Table G-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

G.5 Data Access Events

Data access events track audited Transact-SQL commands, such as all `SELECT TABLE`, `INSERT TABLE`, or `UPDATE TABLE` commands.

The Data Access Report uses these events.

Table G-4 lists the Sybase ASE data access events and the equivalent Oracle Audit Vault and Database Firewall events.

Table G-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

See Also:

Data Access Report

G.6 Exception Events

Exception events track audited error and exception activity, such as network errors.

Table G-5 lists Sybase ASE exception events and the equivalent Oracle AVDF events.

Table G-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

G.7 Invalid Record Events

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

G.8 Object Management Events

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

Table G-6 lists the Sybase ASE object management events and the equivalent Oracle AVDF events.

Table G-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 Object Access Schema Access User Access Password	ACCESS	DATABASE OBJECT SCHEMA USER 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

G.9 Peer Association Events

Peer association events track database link commands. These events do not have any event names.

G.10 Role and Privilege Management Events

Role and privilege management events track audited role and privilege management activity, such as revoking permissions from a user to use a specified command.

Table G-7 lists the Sybase ASE role and privilege management events and the equivalent Oracle AVDF events.

Table G-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
ROLE LOCK	Role Lock	LOCK	ROLE
ROLE TOGGLING	Role Toggling	SET	ROLE
USER-DEFINED FUNCTION COMMAND	Alter Role Function Executed Create Role Function Executed Drop Role Function Executed Grant Role Function Executed Revoke Role Function Executed	ALTER CREATE DROP GRANT REVOKE	ROLE ROLE ROLE ROLE ROLE

G.11 Service and Application Utilization Events

Service and application utilization events track audited application access activity, such as the execution of Transact-SQL commands.

Table G-8 lists the Sybase ASE service and application utilization events and the equivalent Oracle AVDF events.

Table G-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

G.12 System Management Events

System management events track audited system management activity, such as the CREATE DATABASE and DISK INIT commands.

Table G-9 lists the Sybase ASE system management events and the equivalent Oracle AVDF events.

Table G-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

Table G-9 (Cont.) Sybase ASE System Management Audit Events

Source Event	Event Description	Command Class	Target Type
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
JCS INSTALL COMMAND	JCS Install Command	INSTALL	JCS
JCS REMOVE COMMAND	JCS Remove Command	UNINSTALL	JCS
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

G.13 Unknown or Uncategorized Events

Unknown or uncategorized events track audited activity that cannot be categorized.

Table G-10 shows the Sybase ASE unknown or uncategorized event and the equivalent Oracle AVDF event.

Table G-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`

G.14 User Session Events

User session events track audited authentication events for users who log in to the database.

Table G-11 lists the Sybase ASE user session events and the equivalent Oracle AVDF events.

Table G-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`

H

Microsoft SQL Server SQL Trace Audit Events

Microsoft SQL Server SQL trace audit events cover categories such as account management events and application management events.

H.1 About the Microsoft SQL Server Audit Events

The Microsoft SQL Server audit events include categories such as account management events and application management 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 Audit Vault and Database Firewall 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 for Oracle Audit Vault and Database Firewall data warehouse details that may be useful in designing your own reports.

H.2 Account Management Events

Account management events track SQL statements that affect user accounts, such as adding logins or changing login passwords.

Table H-1 lists the Microsoft SQL Server account management events and the equivalent Oracle Audit Vault and Database Firewall events.

Table H-1 Microsoft 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 possible target type values associated with certain SQL Trace Audit Events.
`DATABASE PRINCIPAL MANAGEMENT:CREATE: USER`		`CREATE`	
`DATABASE PRINCIPAL MANAGEMENT:DROP: USER`		`DROP`	

Table H-1 (Cont.) Microsoft SQL Server Account Management Events

Source Event	Event Description	Command Class	Target Type
`LOGIN CHANGE PASSWORD:PASSWORD CHANGED`	Audit Login Change Password Event	`ALTER`	Any possible target type values associated with certain SQL Trace Audit Events.
`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 possible target type values associated with certain SQL Trace Audit Events.
`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 possible target type values associated with certain SQL Trace Audit Events.
`SERVER PRINCIPAL MANAGEMENT:DISABLE`		`DROP`	
`SERVER PRINCIPAL MANAGEMENT:ENABLE`		`ENABLE`	

> **See Also:**
>
> Possible Target Types Values Associated With Certain SQL Trace Audit Events

H.3 Application Management Events

Application management events track actions that were performed on the underlying SQL statements, such as creating objects.

Table H-2 lists the Microsoft SQL Server application management events and the equivalent Oracle Audit Vault and Database Firewall events.

Table H-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 possible target type values associated with certain SQL Trace Audit Events.

`SCHEMA OBJECT TAKE OWNERSHIP: OBJECT`
`SCHEMA OBJECT TAKE OWNERSHIP: PROCEDURE`
`SCHEMA OBJECT TAKE OWNERSHIP: TYPE`
`SCHEMA OBJECT TAKE OWNERSHIP: TRIGGER`
	Audit Schema Object Take Ownership Event	`ALTER`
		`ALTER`
		`ALTER`
		`ALTER`
			Any possible target type values associated with certain SQL Trace Audit Events.

`SERVER OBJECT TAKE OWNERSHIP: OBJECT`	Audit Server Object Take Ownership Event	`ALTER`	Any possible target type values associated with certain SQL Trace Audit Events.

`OBJECT:CREATED:PROCEDURE`
`OBJECT:CREATED:TRIGGER`
`OBJECT:CREATED:TYPE`
`OBJECT:CREATED:BEGIN`
`OBJECT:CREATED:COMMIT`
`OBJECT:CREATED:ROLLBACK`
`OBJECT:DELETED:BEGIN`
	Object:Created
	Object:Deleted
		`CREATE`
		`CREATE`
		`CREATE`
		`COMMIT`
		`ROLLBACK`
		`DROP`
			Any possible target type values associated with certain SQL Trace Audit Events.

`OBJECT:DELETED:PROCEDURE` `OBJECT:DELETED:TRIGGER`	Object:Deleted	`DROP` `DROP`	Any possible target type values associated with certain SQL Trace Audit Events.

See Also:

Possible Target Types Values Associated With Certain SQL Trace Audit Events

H.4 Audit Command Events

Audit command events track the use of audit events, such as altering trace events.

Table H-3 lists the Microsoft SQL Server audit command events and the equivalent Oracle Audit Vault and Database Firewall events.

Table H-3 SQL Server Audit Command Audit Events

Source Event	Event Description	Command Class	Target Type
CHANGE:AUDIT STARTED CHANGE:AUDIT STOPPED CHANGE:C2 MODE ON CHANGE:C2 MODE OFF CHANGE:AUDIT STOPPED CHANGE:NEW AUDIT STARTED	Audit Change Audit Event	AUDIT NOAUDIT AUDIT NOAUDIT SYSTEM SYSTEM	Any possible target type values associated with certain SQL Trace Audit Events.
SERVER ALTER TRACE	Audit Server Alter Trace Event	ALTER	TRACE
EXISTINGCONNECTION	ExistingConnection	EXISTING	Any possible target type values associated with certain SQL Trace Audit Events.

Table H-4 lists the Microsoft SQL Server audit command events that are logged in the Windows Event Viewer.

Table H-4 SQL Server Audit Command Events Logged in Windows Event Viewer

Source Event	Severity
OP ALTER TRACE: START	10
OP ALTER TRACE: STOP	10

> **Note:**
>
> Possible Target Types Values Associated With Certain SQL Trace Audit Events

H.5 Data Access Events

The data access event tracks SQL transactions. The Data Access Report uses these events.

Table H-5 shows the Microsoft SQL Server data access source event and the equivalent Oracle Audit Vault and Database Firewall event.

Table H-5 SQL Server Data Access Audit Event

Source Event	Event Description	Command Class	Target Type
SQL TRANSACTION:BEGIN	SQL Transaction	TRANSACTION MANAGEMENT	TRANSACTION
BATCH COMPLETED	SQL transaction batch completed	EXECUTE	DATABASE

Table H-5 (Cont.) SQL Server Data Access Audit Event

Source Event	Event Description	Command Class	Target Type
BATCH_COMPLETED_GROUP	SQL transaction batch completed	EXECUTE	DATABASE

See Also:

Data Access Report

H.6 Exception Events

Exception events track audited error and exception activity, such as background job errors.

Table H-6 lists the Microsoft SQL Server exception events and the equivalent Oracle Audit Vault and Database Firewall events.

Table H-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:BACKGROUND JOB DROPPED - QUEUE IS FULL BACKGROUND JOB ERROR:BACKGROUND JOB RETURNED AN ERROR	Background Job Error	RAISE RAISE RAISE	Any possible target type values associated with certain SQL Trace Audit Events.
BLOCKED PROCESS REPORT	Blocked Process Report	RAISE	Any possible target type values associated with certain SQL Trace Audit Events.

Table H-7 lists the Microsoft SQL Server exception events that are logged in the Windows Event Viewer.

Table H-7 SQL Server Exception Events Logged in the Windows Event Viewer

Source Event	Severity	command_class	target_type
OP ERROR: COMMIT	10	ERROR	Any possible target type values associated with certain SQL Trace Audit Events.

Table H-7 (Cont.) SQL Server Exception Events Logged in the Windows Event Viewer

Source Event	Severity	command_class	target_type
`OP ERROR: DB OFFLINE`	`10`	`ERROR`	Any possible target type values associated with certain SQL Trace Audit Events.
`OP ERROR: MIRRORING ERROR`	`16`	`ERROR`	Any possible target type values associated with certain SQL Trace Audit Events.
`OP ERROR: .NET FATAL ERROR`	`16`	`ERROR`	Any possible target type values associated with certain SQL Trace Audit Events.
`OP ERROR: .NET USER CODE`	`16`	`ERROR`	Any possible target type values associated with certain SQL Trace Audit Events.
`OP ERROR: PROCESS VIOLATION`	`16`	`ERROR`	Any possible target type values associated with certain SQL Trace Audit Events.
`OP ERROR: RECOVER`	`21`	`ERROR`	Any possible target type values associated with certain SQL Trace Audit Events.
`OP ERROR: RESTORE FAILED`	`21`	`ERROR`	Any possible target type values associated with certain SQL Trace Audit Events.
`OP ERROR: ROLLBACK`	`10`	`ERROR`	Any possible target type values associated with certain SQL Trace Audit Events.
`OP ERROR: SERVER SHUT DOWN`	`21`	`ERROR`	Any possible target type values associated with certain SQL Trace Audit Events.
`OP ERROR: STACK OVER FLOW`	`16`	`ERROR`	Any possible target type values associated with certain SQL Trace Audit Events.

See Also:

Possible Target Types Values Associated With Certain SQL Trace Audit Events

H.7 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.

H.8 Object Management Events

Object management events track audited actions performed on database objects, such as altering an object.

Table H-8 lists the Microsoft SQL Server object management events and the equivalent Oracle Audit Vault and Database Firewall events.

Table H-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 possible target type values associated with certain SQL Trace Audit Events.
`DATABASE OBJECT MANAGEMENT:ACCESS`	Audit Database Object Management Event	`ACCESS`	Any possible target type values associated with certain SQL Trace Audit Events.

`DATABASE OBJECT TAKE OWNERSHIP: OBJECT`
`DATABASE OBJECT TAKE OWNERSHIP: SCHEMA`
	Audit Database Object Take Ownership Event	`ALTER`
		`ALTER`
			Any possible target type values associated with certain SQL Trace Audit Events.

`DATABASE PRINCIPAL MANAGEMENT:CREATE`
`DATABASE PRINCIPAL MANAGEMENT:ALTER`
`DATABASE PRINCIPAL MANAGEMENT:DROP`
	Audit Database Principal Management Event	`CREATE`
		`ALTER`
		`DROP`
			Any possible target type values associated with certain SQL Trace Audit Events.

`SCHEMA OBJECT ACCESS`	Audit Schema Object Access Event	`ACCESS`	Any possible target type values associated with certain SQL Trace Audit Events.

Table H-8 (Cont.) SQL Server Object Management Audit Events

Source Event	Event Description	Command Class	Target Type
SCHEMA OBJECT MANAGEMENT:CREATE SCHEMA OBJECT MANAGEMENT:ALTER SCHEMA OBJECT MANAGEMENT:DROP SCHEMA OBJECT MANAGEMENT:TRANSFER	Audit Schema Object Management Event	CREATE ALTER DROP TRANSFER	Any possible target type values associated with certain SQL Trace Audit Events.
SCHEMA OBJECT TAKE OWNERSHIP: INDEX SCHEMA OBJECT TAKE OWNERSHIP: OBJECT SCHEMA OBJECT TAKE OWNERSHIP: TABLE	Audit Schema Object Take Ownership Event	ALTER ALTER ALTER	Any possible target type values associated with certain SQL Trace Audit Events.
SERVER OBJECT TAKE OWNERSHIP: OBJECT	Audit Server Object Take Ownership Event	ALTER	Any possible target type values associated with certain SQL Trace Audit Events.
LOCK:DEADLOCK	Lock:Deadlock	DEADLOCK	Any possible target type values associated with certain SQL Trace Audit Events.
LOCK:DEADLOCK CHAIN LOCK:DEADLOCK CHAIN:RESOURCE TYPE LOCK	Lock:Deadlock Chain	DEADLOCK DEADLOCK	Any possible target type values associated with certain SQL Trace Audit Events.
OBJECT:ALTERED OBJECT:ALTERED:COMMIT OBJECT:ALTERED:INDEX OBJECT:ALTERED:PROCEDURE OBJECT:ALTERED:ROLLBACK OBJECT:ALTERED:TABLE OBJECT:ALTERED:TRIGGER OBJECT:ALTERED:TYPE OBJECT:ALTERED:BEGIN	Object:Altered	ALTER COMMIT ALTER ALTER ROLLBACK ALTER ALTER ALTER ALTER	Any possible target type values associated with certain SQL Trace Audit Events.
OBJECT:CREATED OBJECT:CREATED:COMMIT OBJECT:CREATED:INDEX OBJECT:CREATED:PROCEDURE OBJECT:CREATED:ROLLBACK OBJECT:CREATED:SCHEMA OBJECT:CREATED:SYNONYM OBJECT:CREATED:TABLE OBJECT:CREATED:TRIGGER OBJECT:CREATED:TYPE OBJECT:CREATED:VIEW	Object:Created	CREATE COMMIT CREATE CREATE ROLLBACK CREATE CREATE CREATE CREATE CREATE CREATE	Any possible target type values associated with certain SQL Trace Audit Events.

Table H-8 (Cont.) SQL Server Object Management Audit Events

Source Event	Event Description	Command Class	Target Type
OBJECT:DELETED	Object:Deleted	DROP	Any possible target type values associated with certain SQL Trace Audit Events.
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	

See Also:

Possible Target Types Values Associated With Certain SQL Trace Audit Events

H.9 Peer Association Events

Peer association events track database link statements.

These events do not have any event names; they only contain event attributes.

H.10 Role and Privilege Management Events

Role and privilege management events track audited role and privilege management activity, such as granting a user access permission.

Table H-9 lists the Microsoft SQL Server role and privilege management events and the equivalent Oracle Audit Vault and Database Firewall events.

Table H-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

Table H-9 (Cont.) SQL Server Role and Privilege Management Audit Events

Source Event	Event Description	Command Class	Target Type
ADD MEMBER TO DB ROLE:ADD ADD MEMBER TO DB ROLE:CHANGE GROUP ADD MEMBER TO DB ROLE:DROP	Audit Add Member to DB Role Event	GRANT ALTER REVOKE	ROLE ROLE ROLE
ADD ROLE:ADD ADD ROLE:DROP	Audit Add Role Event	CREATE DROP	ROLE ROLE
APP ROLE CHANGE PASSWORD	Audit App Role Change Password Event	ALTER	Any possible target type values associated with certain SQL Trace Audit Events.
DATABASE OBJECT GDR:DENY DATABASE OBJECT GDR:GRANT DATABASE OBJECT GDR:REVOKE	Audit Database Object GDR Event	ALTER ALTER ALTER	Any possible target type values associated with certain SQL Trace Audit Events.
DATABASE PRINCIPAL MANAGEMENT:ALTER: ROLE DATABASE PRINCIPAL MANAGEMENT:CREATE: ROLE DATABASE PRINCIPAL MANAGEMENT:DROP: ROLE	Audit Database Principal Management Event	ALTER CREATE DROP	Any possible target type values associated with certain SQL Trace Audit Events.
LOGIN GDR:DENY LOGIN GDR:GRANT LOGIN GDR:REVOKE	Audit Login GDR Event	DENY GRANT REVOKE	Any possible target type values associated with certain SQL Trace Audit Events.
OBJECT DERIVED PERMISSION:CREATE OBJECT DERIVED PERMISSION:ALTER OBJECT DERIVED PERMISSION:DROP OBJECT DERIVED PERMISSION:DUMP OBJECT DERIVED PERMISSION:LOAD	Audit Object Derived Permission Event	CREATE ALTER DROP BACKUP RESTORE	Any possible target type values associated with certain SQL Trace Audit Events.
SCHEMA OBJECT GDR:GRANT SCHEMA OBJECT GDR:REVOKE SCHEMA OBJECT GDR:DENY	Audit Schema Object GDR Event	GRANT REVOKE DENY	OBJECT OBJECT OBJECT
OBJECT PERMISSION	Audit Object Derived Permission Event	CHECK	Any possible target type values associated with certain SQL Trace Audit Events.
SERVER OBJECT GDR:GRANT SERVER OBJECT GDR:REVOKE SERVER OBJECT GDR:DENY	Audit Server Object GDR Event	ALTER ALTER ALTER	Any possible target type values associated with certain SQL Trace Audit Events.
SERVER SCOPE GDR:DENY SERVER SCOPE GDR:GRANT SERVER SCOPE GDR:REVOKE	Audit Server Scope GDR Event	DENY GRANT REVOKE	Any possible target type values associated with certain SQL Trace Audit Events.
DATABASE SCOPE GDR:GRANT STATEMENT GDR:REVOKE STATEMENT GDR:DENY	Audit Database Scope GDR Event	GRANT REVOKE DENY	Any possible target type values associated with certain SQL Trace Audit Events.

Table H-9   (Cont.) SQL Server Role and Privilege Management Audit Events

Source Event	Event Description	Command Class	Target Type
`STATEMENT PERMISSION`	Audit Statement Permission Event	`VALIDATE`	Any possible target type values associated with certain SQL Trace Audit Events.

See Also:

Possible Target Types Values Associated With Certain SQL Trace Audit Events

H.11 Service and Application Utilization Events

Service and application utilization events track audited application access activity.

Table H-10 lists the Microsoft SQL Server service and application utilization events and the equivalent Oracle Audit Vault and Database Firewall events.

Table H-10   SQL Server Service and Application Utilization Audit Events

Source Event	Event Description	Command Class	Target Type

`BROKER CONVERSATION:INVALID SIGNATURE`
`BROKER CONVERSATION:NO CERTIFICATE`
`BROKER CONVERSATION:NO SECURITY HEADER`
`BROKER CONVERSATION:RUN AS TARGET FAILURE`
	Audit Broker Conversation	`EXECUTE`	Any possible target type values associated with certain SQL Trace Audit Events.

`BROKER:MESSAGE UNDELIVERABLE:SEQUENCED`
`BROKER:MESSAGE UNDELIVERABLE:UNSEQUENCED`
`BROKER:MESSAGE UNDELIVERABLE:CORRUPTED MESSAGE`
	Broker:Message Undeliverable
	Broker:Message Undeliverable
	Broker:Corrupted Message
		`TRANSACTION MANAGEMENT`
		`TRANSACTION MANAGEMENT`
		`RECEIVE`
			`MESSAGE`
			`MESSAGE`
			Any possible target type values associated with certain SQL Trace Audit Events.

`BROKER:ACTIVATION:ABORTED`	Broker:Activation - The activation stored procedure exited with an error.	`END`	Any possible target type values associated with certain SQL Trace Audit Events.

Table H-10 (Cont.) SQL Server Service and Application Utilization Audit Events

Source Event	Event Description	Command Class	Target Type
BROKER:QUEUE DISABLED	Broker:Queue Disabled	DISABLE	Any possible target type values associated with certain SQL Trace Audit Events.
RPC STARTED	Remote procedure call	EXECUTE	DATABASE
RPC COMPLETED	Remote procedure call	EXECUTE	DATABASE

> **See Also:**
>
> Possible Target Types Values Associated With Certain SQL Trace Audit Events

H.12 System Management Events

System management events track audited system management activity, such as backup and restore operations.

Table H-11 lists the Microsoft SQL Server system management events and the equivalent Oracle Audit Vault and Database Firewall events.

Table H-11 SQL Server System Management Audit Events

Source Event	Event Description	Command Class	Target Type
ADD DB USER:ADD ADD DB USER:DROP ADD DB USER:SP_ADDUSER ADD DB USER:SP_DROPUSER	Audit Add DB User Event	ALTER ALTER ALTER ALTER	DATABASE DATABASE DATABASE DATABASE
BACKUP/RESTORE:BACKUP BACKUP/RESTORE:BACKUPLOG BACKUP/RESTORE:RESTORE	Audit Backup/Restore Event	BACKUP BACKUP RESTORE	Any possible target type values associated with certain SQL Trace Audit Events.
CHANGE DATABASE OWNER	Audit Change Database Owner	ALTER	Any possible target type values associated with certain SQL Trace Audit Events.

Table H-11 (Cont.) SQL Server System Management Audit Events

Source Event	Event Description	Command Class	Target Type
DATABASE MANAGEMENT:ALTER DATABASE MANAGEMENT:CREATE DATABASE MANAGEMENT:DROP DATABASE MANAGEMENT:DUMP DATABASE MANAGEMENT:LOAD	Audit Database Management Event	ALTER CREATE DROP BACKUP RESTORE	Any possible target type values associated with certain SQL Trace Audit Events.
DATABASE OBJECT MANAGEMENT:ALTER DATABASE OBJECT MANAGEMENT:CREATE DATABASE OBJECT MANAGEMENT:DROP DATABASE OBJECT MANAGEMENT:DUMP DATABASE OBJECT MANAGEMENT:LOAD DATABASE OBJECT MANAGEMENT:OPEN	Audit Database Object Management Event	ALTER ALTER ALTER BACKUP RESTORE ALTER	Any possible target type values associated with certain SQL Trace Audit Events.
DATABASE OPERATION:SUBSCRIBE TO QUERY NOTIFICATION	Audit Database Operation Event	SUBSCRIBE	Any possible target type values associated with certain SQL Trace Audit Events.
DATABASE PRINCIPAL MANAGEMENT:DUMP DATABASE PRINCIPAL MANAGEMENT:LOAD	Audit Database Principal Management Event	BACKUP RESTORE	Any possible target type values associated with certain SQL Trace Audit Events.
DB CONSISTENCY CHECK	Audit DBCC Event	VERIFY	Any possible target type values associated with certain SQL Trace Audit Events.
SCHEMA OBJECT MANAGEMENT:DUMP SCHEMA OBJECT MANAGEMENT:LOAD	Audit Schema Object Management Event	BACKUP RESTORE	Any possible target type values associated with certain SQL Trace Audit Events.

Table H-11 (Cont.) SQL Server System Management Audit Events

Source Event	Event Description	Command Class	Target Type
SERVER OBJECT MANAGEMENT:CREATE SERVER OBJECT MANAGEMENT:ALTER SERVER OBJECT MANAGEMENT:DROP SERVER OBJECT MANAGEMENT:DUMP SERVER OBJECT MANAGEMENT:LOAD	Audit Server Object Management Event	ALTER ALTER ALTER BACKUP RESTORE	SYSTEM SYSTEM SYSTEM Any possible target type values associated with certain SQL Trace Audit Events.
SERVER OPERATION:ADMINISTER BULK OPERATIONS SERVER OPERATION:ALTER RESOURCES SERVER OPERATION:ALTER SERVER STATE SERVER OPERATION:ALTER SETTINGS SERVER OPERATION:AUTHENTICATE SERVER OPERATION:EXTERNAL ACCESS	Audit Server Operation Event	UPDATE UPDATE UPDATE UPDATE UPDATE UPDATE	Any possible target type values associated with certain SQL Trace Audit Events.
SERVER PRINCIPAL MANAGEMENT:DUMP: USER SERVER PRINCIPAL MANAGEMENT:LOAD: USER	Audit Server Principal Management Event	BACKUP RESTORE	Any possible target type values associated with certain SQL Trace Audit Events.
SERVER STARTS AND STOPS:SHUTDOWN SERVER STARTS AND STOPS:STARTED SERVER STARTS AND STOPS:PAUSED SERVER STARTS AND STOPS:CONTINUE	Audit Server Starts and Stops	STOP START SUSPEND RESUME	Any possible target type values associated with certain SQL Trace Audit Events.
SERVER STARTS AND STOPS:INSTANCE CONTINUED SERVER STARTS AND STOPS:INSTANCE PAUSE SERVER STARTS AND STOPS:INSTANCE SHUTDOWN SERVER STARTS AND STOPS:INSTANCE STARTED	Audit Server Starts and Stops Event	RESUME SUSPEND SHUTDOWN STARTUP	Any possible target type values associated with certain SQL Trace Audit Events.
DATABASE MIRRORING STATE CHANGE	Database Mirroring State Change	UPDATE	Any possible target type values associated with certain SQL Trace Audit Events.

Table H-11 (Cont.) SQL Server System Management Audit Events

Source Event	Event Description	Command Class	Target Type
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 possible target type values associated with certain SQL Trace Audit Events.
MOUNT TAPE:TAPE MOUNT COMPLETE		MOUNT	
MOUNT TAPE:TAPE MOUNT REQUEST		MOUNT	
DATABASE BULK ADMIN	DB Bulk administration	INSERT	DATABASE

See Also:

Possible Target Types Values Associated With Certain SQL Trace Audit Events

H.13 Unknown or Uncategorized Events

Unknown or uncategorized events track audited activity that cannot be categorized, such as user-created configurations.

Table H-12 Uncategorised Events

Source Event	Event Description	Command Class	Target Type
ATTENTION	Attention	RAISE	Any possible target type values associated with certain SQL Trace Audit Events.
ERROR LOG	ErrorLog	WRITE	Any possible target type values associated with certain SQL Trace Audit Events.
EXCEPTION	Exception	RAISE	Any possible target type values associated with certain SQL Trace Audit Events.

Table H-12 (Cont.) Uncategorised Events

Source Event	Event Description	Command Class	Target Type
OLEDB ERRORS	OLEDB Errors	RAISE	Any from Possible Target Types Values Associated With Certain SQL Trace Audit Events
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 possible target type values associated with certain SQL Trace Audit Events.
MISSING JOIN PREDICATE	Missing Join Predicate	ACCESS	Any possible target type values associated with certain SQL Trace Audit Events.
SERVER MEMORY CHANGE:INCREASE	Server Memory Change	UPDATE	MEMORY
SERVER MEMORY CHANGE:DECREASE	Server Memory Change	UPDATE	MEMORY
USER ERROR MESSAGE	User Error Message	RAISE	Any possible target type values associated with certain SQL Trace Audit Events.
BITMAP WARNING:DISABLED	Bitmap Warning	RAISE	WARNING
TRACE START	Trace Start	START	Any possible target type values associated with certain SQL Trace Audit Events.
TRACE STOP	Trace Stop	STOP	Any possible target type values associated with certain SQL Trace Audit Events.
SQL:STMTCOMPLETED	SQL:Stmt Completed Event	EXECUTE	Any possible target type values associated with certain SQL Trace Audit Events.
DBCC	Audit DBCC Event	EXECUTE	Any possible target type values associated with certain SQL Trace Audit Events.

Table H-12 (Cont.) Uncategorised Events

Source Event	Event Description	Command Class	Target Type
`SERVER OPERATION:ALTER SERVER STATE`	Audit Server Operation Event	`UPDATE`	Any possible target type values associated with certain SQL Trace Audit Events.
`LOCK:DEADLOCK CHAIN:RESOURCE TYPE LOCK`	Lock:Deadlock Chain	`DEADLOCK`	Any possible target type values associated with certain SQL Trace Audit Events.
`USER CONFIGURABLE`	User Configurable (Event ID:82)	`CONFIGURE`	Any possible target type values associated with certain SQL Trace Audit Events.
`USER CONFIGURABLE`	User Configurable (Event ID:83)	`CONFIGURE`	Any possible target type values associated with certain SQL Trace Audit Events.
`USER CONFIGURABLE`	User Configurable (Event ID:84)	`CONFIGURE`	Any possible target type values associated with certain SQL Trace Audit Events.
`USER CONFIGURABLE`	User Configurable (Event ID:85)	`CONFIGURE`	Any possible target type values associated with certain SQL Trace Audit Events.
`USER CONFIGURABLE`	User Configurable (Event ID:86)	`CONFIGURE`	Any possible target type values associated with certain SQL Trace Audit Events.
`USER CONFIGURABLE`	User Configurable (Event ID:87)	`CONFIGURE`	Any possible target type values associated with certain SQL Trace Audit Events.
`USER CONFIGURABLE`	User Configurable (Event ID:88)	`CONFIGURE`	Any possible target type values associated with certain SQL Trace Audit Events.
`USER CONFIGURABLE`	User Configurable (Event ID:89)	`CONFIGURE`	Any possible target type values associated with certain SQL Trace Audit Events.

Table H-12 (Cont.) Uncategorised Events

Source Event	Event Description	Command Class	Target Type
USER CONFIGURABLE	User Configurable (Event ID:90)	CONFIGURE	Any possible target type values associated with certain SQL Trace Audit Events.
USER CONFIGURABLE	User Configurable (Event ID:91)	CONFIGURE	Any possible target type values associated with certain SQL Trace Audit Events.
NOTIFICATION SERVICE	Notification Service	RAISE	DATABASE
PASSWORD POLICY	Password Policy	UPDATE	POLICY

> **See Also:**
>
> Possible Target Types Values Associated With Certain SQL Trace Audit Events

H.14 User Session Events

User session events track audited authentication events for users who log in to the database.

Table H-13 lists the Microsoft SQL Server user session events and the equivalent Oracle Audit Vault and Database Firewall events.

Table H-13 SQL Server User Session Audit Events

Source Event	Event Description	Command Class	Target Type
BROKER LOGIN:AUTHENTICATION FAILURE BROKER LOGIN:LOGIN SUCCESS BROKER LOGIN:LOGIN PROTOCOL ERROR BROKER LOGIN:MESSAGE FORMAT ERROR BROKER LOGIN:NEGOTIATE FAILURE	Audit Broker Login	LOGIN LOGIN LOGIN LOGIN LOGIN	Any possible target type values associated with certain SQL Trace Audit Events.
DATABASE MIRRORING LOGIN:LOGIN SUCCESS 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	Audit Database Mirroring Login Event	LOGIN	Any possible target type values associated with certain SQL Trace Audit Events.

Table H-13 (Cont.) SQL Server User Session Audit Events

Source Event	Event Description	Command Class	Target Type
DATABASE OPERATION:CHECKPOINT	Audit Database Operation Event	SAVEPOINT	Any possible target type values associated with certain SQL Trace Audit Events.
DATABASE PRINCIPAL IMPERSONATION	Audit Database Principal Impersonation Event	IMPERSONATION	Any possible target type values associated with certain SQL Trace Audit Events.
LOGIN:NONPOOLED LOGIN:POOLED LOGIN:FAILED LOGOUT:NONPOOLED LOGOUT:POOLED LOGIN FAILED:NONPOOLED LOGIN FAILED:POOLED	Audit Login Audit Login Audit Login Failed Audit Logout Audit Logout Login Failed Event Login Failed Event	LOGIN LOGIN LOGIN LOGOUT LOGOUT LOGIN LOGIN	USER USER Any possible target type values associated with certain SQL Trace Audit Events. USER USER USER USER
SERVER PRINCIPAL IMPERSONATION	Audit Server Principal Impersonation Event	IMPERSONATION	Any possible target type values associated with certain SQL Trace Audit Events.
SQL TRANSACTION:COMMIT SQL TRANSACTION:ROLLBACK SQL TRANSACTION:SAVEPOINT	SQL Transaction	COMMIT ROLLBACK SAVEPOINT	Any possible target type values associated with certain SQL Trace Audit Events.
TRANSACTION BEGIN COMPLETED	SQL Transaction	EXECUTE	DATABASE
TRANSACTION BEGIN STARTING	SQL Transaction	EXECUTE	DATABASE
TRANSACTION COMMIT COMPLETED	SQL Transaction	EXECUTE	DATABASE
TRANSACTION COMMIT STARTING	SQL Transaction	EXECUTE	DATABASE
TRANSACTION PROMOTE COMPLETED	SQL Transaction	EXECUTE	DATABASE
TRANSACTION PROMOTE STARTING	SQL Transaction	EXECUTE	DATABASE
TRANSACTION PROPAGATE COMPLETED	SQL Transaction	EXECUTE	DATABASE
TRANSACTION PROPAGATE STARTING	SQL Transaction	EXECUTE	DATABASE
TRANSACTION ROLLBACK COMPLETED	SQL Transaction	EXECUTE	DATABASE
TRANSACTION ROLLBACK STARTING	SQL Transaction	EXECUTE	DATABASE
TRANSACTION SAVEPOINT COMPLETED	SQL Transaction	EXECUTE	DATABASE
TRANSACTION SAVEPOINT STARTING	SQL Transaction	EXECUTE	DATABASE
STORAGE LOGIN	Storage login	LOGIN	SERVER

Table H-13 (Cont.) SQL Server User Session Audit Events

Source Event	Event Description	Command Class	Target Type
STORAGE_LOGIN_GROUP	Storage login	LOGIN	SERVER

> **See Also:**
>
> Possible Target Types Values Associated With Certain SQL Trace Audit Events

H.15 Target Type Values for SQL Trace Audit Events

Target Type values associated with certain audit events.

These events can be any from the following list. See the Audit Event tables in this Appendix for references.

H.16 Possible Target Types Values Associated With Certain SQL Trace Audit Events

There is a large range of target type values that are associated with certain audit events.

```
INDEX
PROCEDURE
TRIGGER
TABLE
VIEW
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
RESOURCE GOVERNOR
DATABASE CONFIGURATION
EXTERNAL LIBRARY
EXTERNAL RESOURCE POOL
EXTERNAL SCRIPT QUERY
```

I

Microsoft SQL Server SQL Audit and Event Log Events

Microsoft SQL Server SQ audit events cover categories such as account management events and application management events.

I.1 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.

> **Note:**
>
> In the table below the **Target Type** can be anything from Possible Target Types Values Associated With SQL Audit and Event Log Events.

Table I-1 SQL Audit Events

Source Event	Event Description	Command Class
DATABASE_ROLE_MEMBER_CHANGE_GROUP	Database Role Member Change Group	ALTER
BACKUP LOG	Backup Log	BACKUP
ALTER RESOURCES	Alter Resources	ALTER
DELETE	Delete	DELETE
BROKER LOGIN	Broker Login	LOGIN
LOGOUT GROUP	Logout Group	LOGOUT
MUST CHANGE PASSWORD	Must Change Password	UPDATE
DROP MEMBER	Drop Member	DROP
DENY	Deny	DENY
SEND	Send	SEND

Table I-1 (Cont.) SQL Audit Events

Source Event	Event Description	Command Class
SELECT	Select	SELECT
SERVER_CONTINUE	Server Continue	RESUME
SERVER OPERATION GROUP	Server Operation Group	EXECUTE
INSERT	Insert	INSERT
EXECUTE	Execute	EXECUTE
SHOW PLAN	Show Plan	EXECUTE
SUCCESSFUL_LOGIN_GROUP	Successful Login Group	LOGIN
SERVER_ROLE_MEMBER_CHANGE_GROUP	Server Role Member Change Group	ALTER
ALTER TRACE	Alter Trace	ALTER
CREDENTIAL MAP TO LOGIN	Credential Map to Login	SET
FULL TEXT	Full Text	EXECUTE
TRACE AUDIT C2ON	Trace Audit C2On	AUDIT
BULK ADMIN	Bulk Admin	INSERT
TRACE AUDIT C2OFF	Trace Audit C2Off	NOAUDIT
VIEW SERVER STATE	View Server State	EXECUTE
SCHEMA_OBJECT_ACCESS_GROUP	Schema Object Access Group	ACCESS
ALTER CONNECTION	Alter Connection	ALTER
ALTER SETTINGS	Alter Settings	ALTER
ALTER SERVER STATE	Alter Server State	ALTER
EXTERNAL ACCESS ASSEMBLY	External Access Assembly	ACCESS
OPEN	Open	OPEN
AUDIT SHUTDOWN ON FAILURE	Audit Shutdown On Failure	NOAUDIT
AUDIT SESSION CHANGED	Audit Session Changed	AUDIT
BACKUP_RESTORE_GROUP	Backup Restore Group	RESTORE
SERVER_OBJECT_OWNERSHIP_CHANGE_GROUP	Server Object Ownership Change Group	ALTER
AUTHENTICATE	Authenticate	AUTHENTICATE
DATABASE_OWNERSHIP_CHANGE_GROUP	Database Ownership Change Group	ALTER
REFERENCES	References	ACCESS
SERVER_STARTED	Server Started	STARTUP
DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP	Database Object Ownership Change Group	ALTER
SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP	Schema Object Permission Change Group	ALTER
IMPERSONATE	Impersonate	PROXY
CREATE	Create	CREATE
SERVER_STATE_CHANGE_GROUP	Server State Change Group	ALTER

Table I-1 (Cont.) SQL Audit Events

Source Event	Event Description	Command Class
TAKE OWNERSHIP	Take Ownership	ALTER
TRANSFER	Transfer	MOVE
CHANGE USERS LOGIN AUTO	Change Users Login Auto	ALTER
ADD MEMBER	Add Member	UPDATE
VIEW CHANGETRACKING	View ChangeTracking	EXECUTE
LOGIN FAILED	Login Failed	LOGIN
DATABASE_PRINCIPAL_CHANGE_GROUP	Database Principal Change Group	ALTER
DATABASE_OBJECT_CHANGE_GROUP	Database Object Change Group	UPDATE
DATABASE_MIRRORING_LOGIN_GROUP	Database Mirroring Login Group	LOGIN
ALTER	Alter	LOGIN
PASSWORD EXPIRATION	Password Expiration	EXPIRE
UPDATE	Update	UPDATE
NAME CHANGE	Name Change	ALTER
LOGOUT	Logout	LOGOUT
LOGIN SUCCEEDED	Login Succeeded	LOGIN
DATABASE_CHANGE_GROUP	Database Change Group	UPDATE
LOGIN_CHANGE_PASSWORD_GROUP	Login Change Password Group	UPDATE
RESET OWN PASSWORD	Reset Own Password	RESET
CHANGE USERS LOGIN	Change Users Login	ALTER
TRACE_CHANGE_GROUP	Trace Change Group	ALTER
FAILED_LOGIN_GROUP	Failed Login Group	LOGIN
TRACE AUDIT STOP	Trace Audit Stop	NOAUDIT
REVOKE	Revoke	REVOKE
CHANGE OWN PASSWORD	Change Own Password	UPDATE
CHANGE LOGIN CREDENTIAL	Change Login Credential	ALTER
RECEIVE	Receive	GET
AUDIT_CHANGE_GROUP	Audit Change Group	AUDIT
CHANGE DEFAULT LANGUAGE	Change Default Language	ALTER
CHANGE PASSWORD	Change Password	UPDATE
RESTORE	Restore	RESTORE
DATABASE MIRRORING LOGIN	Database Mirroring Login	LOGIN
REVOKE WITH CASCADE	Revoke with Cascade	REVOKE
DROP	Drop	DROP
SERVER_OBJECT_CHANGE_GROUP	Server Object Change Group	ALTER
VIEW_DATABASE_STATE	View Database State	EXECUTE
SERVER_PRINCIPAL_CHANGE_GROUP	Server Principal Change Group	ALTER

Table I-1 (Cont.) SQL Audit Events

Source Event	Event Description	Command Class
UNLOCK ACCOUNT	Unlock Account	UNLOCK
FULLTEXT_GROUP	Fulltext Group	EXECUTE
ENABLE	Enable	ENABLE
PASSWORD POLICY	Password Policy	UPDATE
REVOKE WITH GRANT	Revoke With Grant	REVOKE
DATABASE_PRINCIPAL_IMPERSONATION_GROUP	Database Principal Impersonation Group	PROXY
RESET PASSWORD	Reset Password	RESET
SUBSCRIBE QUERY NOTIFICATION	Subscribe Query Notification	SUBSCRIBE
SERVER_PRINCIPAL_IMPERSONATION_GROUP	Server Principal Impersonation Group	PROXY
APPLICATION_ROLE_CHANGE_PASSWORD_GROUP	Application Role Change Password Group	UPDATE
TRACE AUDIT START	Trace Audit Start	AUDIT
DATABASE OBJECT PERMISSION CHANGE GROUP	Database Object Permission Change Group	ALTER
SERVER PAUSED	Server Paused	PAUSE
DATABASE_OPERATION_GROUP	Database Operation Group	DML
ACCESS	Access	ACCESS
DATABASE_PERMISSION_CHANGE_GROUP	Database Permission Change Group	ALTER
UNSAFE ASSEMBLY	Unsafe Assembly	ACCESS
DENY WITH CASCADE	Deny with Cascade	DENY
DBCC_GROUP	DBCC Group	EXECUTE
BROKER_LOGIN_GROUP	Broker Login Group	LOGIN
CHECKPOINT	Checkpoint	SAVEPOINT
SERVER SHUTDOWN	Server Shutdown	SHUTDOWN
NO CREDENTIAL MAP TO LOGIN	No Credential Map to Login	SET
SCHEMA_OBJECT_CHANGE_GROUP	Schema Object Change Group	ALTER
CONNECT	Connect	CONNECT
GRANT WITH GRANT	Grant with Grant	GRANT
CHANGE DEFAULT DATABASE	Change Default Database	ALTER
DISABLE	Disable	DISABLE
SCHEMA_OBJECT_OWNERSHIP CHANGE_GROUP	Schema Object Ownership Change Group	ALTER
GRANT	Grant	GRANT
SERVER_PERMISSION_CHANGE_GROUP	Server Permission Change Group	ALTER

Table I-1 (Cont.) SQL Audit Events

Source Event	Event Description	Command Class
SERVER_OBJECT_PERMISSION CHANGE_GROUP	Server Object Permission Change Group	ALTER
DATABASE_OBJECT_ACCESS_GROUP	Database Object Access Group	ACCESS
DBCC	DBCC	EXECUTE
BACKUP	Backup	BACKUP
GLOBAL TRANSACTIONS LOGIN	Global Transaction Login	LOGIN
GLOBAL_TRANSACTION_LOGIN_GROUP	Global Transaction Login Group	LOGIN
VIEW	VIEW	EXECUTE

> **See Also:**
>
> Possible Target Types Values Associated With SQL Audit and Event Log Events for the **Target Type**.

I.2 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 I-2 Event Log Events

Source Events	Event Description	Command Class	Target Type
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

Table I-2 (Cont.) Event Log Events

Source Events	Event Description	Command Class	Target Type
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
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

Table I-2 (Cont.) Event Log Events

Source Events	Event Description	Command Class	Target Type
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

I.3 Target Type Values for SQL Audit and Event Log Events

Target Type values associated with certain audit events

These can be any from the following list. See the Audit Event tables in this Appendix for references.

I.4 Possible Target Types Values Associated With SQL Audit and Event Log Events

The possible target type values can be types such as constraints.

Possible Target Types	Class_Type
CONSTRAINT	F
DATABASE	DT
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

Possible Target Types	Class_Type
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
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

Possible Target Types	Class_Type
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
SERVER AUDIT	A
FUNCTION	IF
FUNCTION	IS
TABLE	IT
INDEX	IX
COLUMN ENCRYPTION KEY	CK
COLUMN MASTER KEY DEFINITION	CM
DATABASE CREDENTIAL	DC
EXTERNAL DATA SOURCE	ED
EXTERNAL FILE FORMAT	EF
SECURITY POLICY	SP
SEARCH PROPERTY LIST	FP
SEQUENCE OBJECT	SO
AVAILABILITY GROUP	AG

J
IBM DB2 Audit Events

IBM DB2 audit events cover categories such as account management events and application management events.

J.1 About the IBM DB2 for LUW Audit Events

IBM DB2 for LUW audit events are in categories such as account management events or application management 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 Audit Vault and Database Firewall 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 for Oracle Audit Vault and Database Firewall data warehouse details that may be useful in designing your own reports.

J.2 Account Management Events

Account management events track SQL commands that affect user accounts, such as the `UNLOCK ADMIN ACCOUNT` command.

Table J-1 lists the IBM DB2 account management events and the equivalent Oracle Audit Vault and Database Firewall events.

Table J-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 possible target type values for IBM DB2 Audit Events in List 3.
ALTER_USER_ADD_ROLE	Alter User Add Role	ALTER	NULL
ALTER_USER_ADD_ROLE	Alter User Add Role	ALTER	Any possible target type values for IBM DB2 Audit Events in List 3.

Table J-1 (Cont.) IBM DB2 Account Management Audit Events

Source Event	Event Description	Command Class	Target Type
`ALTER_USER_AUTHENTICATION`	Alter User Authentication	`ALTER`	Any possible target type values for IBM DB2 Audit Events in List 3.
`ALTER_USER_DROP_ROLE`	Alter User Drop Role	`ALTER`	Any possible target type values for IBM DB2 Audit Events in List 3.
`AUTHENTICATION`	Authentication	`VALIDATE`	NULL
`DROP_DEFAULT_ROLE`	Drop Default Role	DROP	NULL
`DROP_USER`	Drop User	`DROP`	Any possible target type values for IBM DB2 Audit Events in List 3.
`SET_SESSION_USER`	Set Session User	`SET`	Any possible target type values for IBM DB2 Audit Events in List 3.

See Also:

List 3: Possible Target Type Values for IBM DB2 Audit Events for possible **Target Type** values.

J.3 Application Management Events

Application management events track actions performed on the underlying SQL commands of system services and applications, such as the `CREATE RULE` command.

Table J-2 lists the IBM DB2 application management events and the equivalent Oracle Audit Vault and Database Firewall events.

Table J-2 IBM DB2 Application Management Events

Source Event	Event Description	Command Class	Target Type
`ALTER_OBJECT`	Alter Object	`ALTER` `ALTER` `ALTER` `ALTER` `ALTER` `ALTER`	Any possible target type values for IBM DB2 Audit Events in List 2.

Table J-2 (Cont.) IBM DB2 Application Management Events

Source Event	Event Description	Command Class	Target Type
CREATE_OBJECT	Create Object	CREATE CREATE CREATE CREATE CREATE CREATE	Any possible target type values for IBM DB2 Audit Events in List 2.
DROP_OBJECT	Drop Object	DROP DROP DROP DROP DROP DROP	Any possible target type values for IBM DB2 Audit Events in List 2.

See Also:

List 2: Possible Target Type Values for IBM DB2 Audit Events

J.4 Audit Command Events

Audit command events track the use of auditing SQL commands on other SQL commands and on database objects.

Table J-3 lists the IBM DB2 audit command events and the equivalent Oracle AVDF events.

Table J-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
DB2AUD	DB2 Aud	ALTER	NULL
DROP_AUDIT_POLICY	Drop Audit Policy	NOAUDIT	POLICY
PRUNE	Prune	GRANT	NULL
START	Start	AUDIT	NULL
STOP	Stop	NOAUDIT	NULL

J.5 Context Events

Context events include start and stop events.

Table J-4 lists the IBM DB2 context events and the equivalent Oracle AVDF events.

Table J-4 IBM DB2 Audit Context Audit Events

Source Event	Event Description	Command Class	Target Type
DARI_START	DARI Start	START	NULL
DARI_STOP	DARI Stop	STOP	NULL
REORG	Reorg	REFRESH	NULL

J.6 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 uses these events.

Table J-5 lists the IBM DB2 data access events and the equivalent Oracle Audit Vault and Database Firewall events.

Table J-5 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

See Also:

Data Access Report

J.7 Exception Events

Exception events track audited error and exception activity, such as network errors.

These events do not have any event names.

J.8 Execution Event

The IBM DB2 execution event is a data event.

Table J-6 lists the IBM DB2 execution event and the equivalent Oracle AVDF event.

Table J-6 IBM DB2 Execution Event

Source Event	Event Description	Command Class	Target Type
`DATA`	A host variable or parameter marker data values for the statement. This event is repeated for each host variable or parameter marker that is part of the statement. It is only present in a delimited extract of an audit log.	`SET`	`NULL`

J.9 Invalid Record Events

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

J.10 Object Management Events

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

Table J-7 lists the IBM DB2 object management events and the equivalent Oracle Audit Vault and Database Firewall events.

Table J-7 IBM DB2 Object Management Audit Events

Source Event	Event Description	Command Class	Target Type
`ALTER_OBJECT`	Alter Object	`ALTER` `ALTER` `ALTER` `ALTER` `ALTER` `ALTER`	Any possible target type values for IBM DB2 Audit Events in List 2.

Table J-7   (Cont.) IBM DB2 Object Management Audit Events

Source Event	Event Description	Command Class	Target Type
CREATE_OBJECT	Create Object	CREATE CREATE CREATE CREATE CREATE CREATE	Any possible target type values for IBM DB2 Audit Events in List 2.
DROP_OBJECT	Drop Object	DROP DROP DROP DROP DROP DROP	Any possible target type values for IBM DB2 Audit Events in List 2.
RENAME_OBJECT	Rename Object	RENAME	Any possible target type values for IBM DB2 Audit Events in List 2.

See Also:

List 2: Possible Target Type Values for IBM DB2 Audit Events

J.11 Peer Association Events

Peer association events track database link commands.

These events do not have any event names; they only contain event attributes.

J.12 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 J-8 lists the IBM DB2 role and privilege management events and the equivalent Oracle Audit Vault and Database Firewall events.

Table J-8   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

Table J-8 (Cont.) IBM DB2 Role and Privilege Management Audit Events

Source Event	Event Description	Command Class	Target Type
ALTER_OBJECT	Alter Object	ALTER	Any from List 2: Possible Target Type Values for IBM DB2 Audit Events
ALTER_SECURITY_POLICY	Alter security policy	ALTER	NULL
CHECKING_FUNCTION	Checking Function	VALIDATE	Any from List 1: Possible Target Type Values for IBM DB2 Audit Events
CHECKING_MEMBERSHIP_IN_ROLES	Checking Membership In Roles	VALIDATE	NULL
CHECKING_OBJECT	Checking Object	VALIDATE	Any from List 1: Possible Target Type Values for IBM DB2 Audit Events
CHECKING_TRANSFER	Checking Transfer	VALIDATE	NULL
CREATE_OBJECT	Create Object	CREATE	Any from List 2: Possible Target Type Values for IBM DB2 Audit Events
DROP_DEFAULT_ROLE	Drop Default Role	DROP	NULL
DROP_OBJECT	Drop Object	DROP	Any from List 2: Possible Target Type Values for IBM DB2 Audit Events
GRANT	Grant	GRANT	Any from List 3: Possible Target Type Values for IBM DB2 Audit Events
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: Possible Target Type Values for IBM DB2 Audit Events
IMPLICIT_REVOKE	Implicit Revoke	REVOKE	Any from List 3: Possible Target Type Values for IBM DB2 Audit Events
REVOKE	Revoke	REVOKE	Any from List 3: Possible Target Type Values for IBM DB2 Audit Events
REVOKE_DB_AUTH	Revoke DB Auth	REVOKE	NULL
REVOKE_DB_AUTHORITIES	Revoke DB Authorities	SYSTEM	NULL
REVOKE_DBADM	Revoke DBADM	REVOKE	NULL

J.13 Service and Application Utilization Events

Service and application utilization events track audited application access activity, such as the execution of SQL commands.

Table J-9 lists the IBM DB2 service and application utilization events and the equivalent Oracle AVDF events.

Table J-9   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

J.14 System Administration Events

System administration events track SQL commands that affect the system administration of a DB2 database, such as commit operations.

Table J-10 lists the IBM DB2 system administration events and the equivalent Oracle AVDF events.

Table J-10   IBM DB2 System Administration Audit Events

Source Event	Event Description	Command Class	Target Type
ATTACH_DEBUGGER	Attach Debugger	LOAD	NULL
COMMIT_DSF_CFS	Commit DSF CFS	COMMIT	NULL
COMMIT_DSF_CM	Commit DSF CM	COMMIT	NULL
COMMIT_DSF_INSTANCE	Commit DSF Instance	COMMIT	NULL
MAINTENANCE_DSF_MODE	Maintenance DSF Mode	UPDATE	NULL
START_CF	Start CF	START	NULL
STOP_CF	Stop CF	STOP	NULL
START_DSF_INSTANCE	Start DSF Instance	START	NULL
STOP_DSF_INSTANCE	Stop DSF Instance	STOP	NULL
TRANSFER_OWNERSHIP	Transfer Ownership	MOVE	NULL
UPDATE_DSF_MEMBER_OR_CF	Update DSF Member or CF	UPDATE	NULL

J.15 System Management Events

System management events track audited system management activity, such as the CREATE DATABASE and DISK INIT commands.

Table J-11 lists the IBM DB2 system management events and the equivalent Oracle AVDF events.

Table J-11 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: Possible Target Type Values for IBM DB2 Audit Events
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: Possible Target Type Values for IBM DB2 Audit Events
CREATE_TABLESPACE	Create Tablespace	CREATE	TABLESPACE
DB2AUDIT	DB2 Audit	ALTER	NULL
DB2REMOT	DB2 Remote	REMOTE CALL	NULL
DB2SET	DB2 Set	ALTER	NULL

Table J-11 (Cont.) IBM DB2 System Management Audit Events

Source Event	Event Description	Command Class	Target Type
DB2TRC	Db2trc	DROP	NULL
DBM_CFG_OPERATION	DBM Cfg Operation	CONFIGURE	NULL
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: Possible Target Type Values for IBM DB2 Audit Events
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

Table J-11 (Cont.) IBM DB2 System Management Audit Events

Source Event	Event Description	Command Class	Target Type
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
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

Table J-11 (Cont.) IBM DB2 System Management Audit Events

Source Event	Event Description	Command Class	Target Type
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
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: Possible Target Type Values for IBM DB2 Audit Events
UPDATE_RECOVERY_HISTORY	Update Recovery History	UPDATE	NULL

J.16 Unknown or Uncategorized Events

Unknown or uncategorized events track audited activity that cannot be categorized.

Table J-12 lists the IBM DB2 unknown or uncategorized event and equivalent Oracle AVDF event.

Table J-12 IBM DB2 Unknown or Uncategorized Audit Events

Source Event	Event Description	Command Class	Target Type
ALTER_OBJECT	Alter Object	ALTER	Any from List 2: Possible Target Type Values for IBM DB2 Audit Events
CREATE_OBJECT	Create Object	CREATE	Any from List 2: Possible Target Type Values for IBM DB2 Audit Events
DROP_OBJECT	Drop Object	DROP	Any from List 2: Possible Target Type Values for IBM DB2 Audit Events

J.17 User Session Events

User session events track audited authentication events for users who log in to the database.

Table J-13 lists the IBM DB2 user session events and the equivalent Oracle AVDF events.

Table J-13   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
SET_SESSION_USER	Set Session User	SET	NULL
SWITCH_USER	Switch User	MOVE	NULL
SWITCH USER	Switch User	MOVE	NULL

J.18 Possible Target Type Values for IBM DB2 Audit Events

Target Type values associated with certain audit events can be from categories such as FUNCTION, MODULE, or INDEX.

See the Audit Event tables in the appendix for references.

J.18.1 List 1: Possible Target Type Values for IBM DB2 Audit Events

Possible target types can be FUNCTION, VARIABLE, and HISTOGRAM TEMPLATE.

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
PROCEDURE
TABLE
TABLESPACE
THRESHOLD
CONTEXT
TYPE MAPPING
TYPE&TRANSFORM
USER MAPPING
VIEW
WORK ACTION SET
WORK CLASS SET
WORKLOAD
WRAPPER
XSR OBJECT
```

J.18.2 List 2: Possible Target Type Values for IBM DB2 Audit Events

Possible target types can include `SYNONYM`, `BUFFERPOOL`, and `EVENT MONITOR`.

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
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
```

J.18.3 List 3: Possible Target Type Values for IBM DB2 Audit Events

Possible target types can be `RULE`, `DATABASE`, and `METHOD`.

Possible Target Types

```
RULE
DATABASE
FUNCTION
VARIABLE
INDEX
METHOD
MODULE
SYNONYM
NONE
PACKAGE
ROLE
SCHEMA
LABEL
POLICY
SERVER
PROCEDURE
TABLE
TABLESPACE
CONTEXT
VIEW
WORKLOAD
```

```
XSR OBJECT
PRIMARY KEY
MASK
USER TEMPORARY TABLE
TRUSTED CONTEXT
PERMISSION
```

K

MySQL Audit Events

MySQL audit events can include events such as BINLOG, CHANGE, and CONNECT,

This appendix maps audit event names used in MySQL to their equivalent values in the **command_class** and **target_type** fields in the Oracle Audit Vault and Database Firewall 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 for Oracle Audit Vault and Database Firewall data warehouse details that may be useful in designing your own reports.

Table K-1 lists the MySQL audit events and the equivalent Oracle Audit Vault and Database Firewall events.

Table K-1 MySQL Audit Events

Source Event	Command Class	Target Type
AUDIT	AUDIT	SYSTEM
BINLOG DUMP	DUMP	TRACE
CHANGE USER	UPDATE	USER
CLOSE STMT	CLOSE	STATEMENT
CONNECT OUT	DISCONNECT	SYSTEM
CONNECT	CONNECT	SYSTEM or DATABASE
CREATE DB	CREATE	DATABASE
DAEMON	EXECUTE	DAEMON
DEBUG	ENABLE	DEBUG
DELAYED INSERT	INSERT	TABLE
DROP DB	DROP	DATABASE
EXECUTE	EXECUTE	STATEMENT
FETCH	RETRIEVE	TABLE
FIELD LIST	RETRIEVE	PROPERTY
INIT DB	INITIALIZE	DATABASE
KILL	KILL	CONNECTION or QUERY
LONG DATA	EXECUTE	STATEMENT
NOAUDIT	NOAUDIT	SYSTEM

Table K-1 (Cont.) MySQL Audit Events

Source Event	Command Class	Target Type
PING	CONNECT	SYSTEM
PREPARE	INITIALIZE	STATEMENT
PROCESSLIST	RETRIEVE	PROCESS
QUERY	EXECUTE	STATEMENT
QUIT	DISCONNECT	SYSTEM
REFRESH	REFRESH	SYSTEM
REGISTER REPLICA	REGISTER	SYSTEM
RESET STMT	RESET	STATEMENT
SET OPTION	SET	VARIABLE
SHUTDOWN	SHUTDOWN	SYSTEM
SLEEP	SLEEP	CONNECTION
STATISTICS	RETRIEVE	STATISTICS
TABLE DUMP	DUMP	TABLE
TIME	RETRIEVE	TIME
ADMIN_COMMANDS	EXECUTE	COMMAND
ASSIGN_TO_KEYCACHE	ASSIGN	TABLE
ALTER_DB	ALTER	DATABASE
ALTER_DB_UPGRADE	UPDATE	DATABASE
ALTER_EVENT	ALTER	EVENT
ALTER_FUNCTION	ALTER	FUNCTION
ALTER_INSTANCE	ALTER	INSTANCE
ALTER_PROCEDURE	ALTER	PROCEDURE
ALTER_SERVER	ALTER	SERVER
ALTER_TABLE	ALTER	TABLE
ALTER_TABLESPACE	ALTER	TABLESPACE
ALTER_USER	ALTER	USER
ANALYZE	ANALYZE	TABLE
BEGIN	START	TRANSACTION
BINLOG	WRITE	TRACE
CALL_PROCEDURE	EXECUTE	PROCEDURE
CHANGE_DB	UPDATE	DATABASE
CHANGE_MASTER	UPDATE	SYSTEM
CHANGE_REPL_FILTER	UPDATE	FILTER
CHECK	VALIDATE	TABLE
CHECKSUM	VALIDATE	TABLE
COMMIT	COMMIT	TRANSACTION

Table K-1 (Cont.) MySQL Audit Events

Source Event	Command Class	Target Type
CREATE_DB	CREATE	DATABASE
CREATE_EVENT	CREATE	EVENT
CREATE_FUNCTION	CREATE	FUNCTION
CREATE_INDEX	CREATE	INDEX
CREATE_PROCEDURE	CREATE	PROCEDURE
CREATE_SERVER	CREATE	SERVER
CREATE_TABLE	CREATE	TABLE
CREATE_TRIGGER	CREATE	TRIGGER
CREATE_UDF	CREATE	FUNCTION
CREATE_USER	CREATE	USER
CREATE_VIEW	CREATE	VIEW
DEALLOC_SQL	DROP	STATEMENT
DELETE	DELETE	TABLE
DELETE_MULTI	DELETE	TABLE
DO	EXECUTE	EXPRESSION
DROP_DB	DROP	DATABASE
DROP_EVENT	DROP	EVENT
DROP_FUNCTION	DROP	FUNCTION
DROP_INDEX	DROP	INDEX
DROP_PROCEDURE	DROP	PROCEDURE
DROP_SERVER	DROP	SERVER
DROP_TABLE	DROP	TABLE
DROP_TRIGGER	DROP	TRIGGER
DROP_USER	DROP	USER
DROP_VIEW	DROP	VIEW
EMPTY_QUERY	EXECUTE	STATEMENT
EXECUTE_SQL	EXECUTE	STATEMENT
EXPLAIN_OTHER	RETRIEVE	TABLE
FLUSH	FLUSH	TABLE or null
GET_DIAGNOSTICS	RETRIEVE	TRACE
GRANT	GRANT	PRIVILEGE
HA_CLOSE	CLOSE	TABLE
HA_OPEN	OPEN	TABLE
HA_READ	READ	TABLE
HELP	GET	SUMMARY
INSERT	INSERT	TABLE

Table K-1 (Cont.) MySQL Audit Events

Source Event	Command Class	Target Type
INSERT_SELECT	INSERT	TABLE
INSTALL_PLUGIN	INSTALL	PLUGIN
LOAD	LOAD	TABLE
LOCK_TABLES	LOCK	TABLE
OPTIMIZE	OPTIMIZE	TABLE
PRELOAD_KEYS	LOAD	TABLE
PREPARE_SQL	INITIALIZE	STATEMENT
PURGE	DROP	TRACE
PURGE_BEFORE_DATE	DROP	TRACE
RELEASE_SAVEPOINT	RELEASE	SAVEPOINT
RENAME_TABLE	RENAME	TABLE
RENAME_USER	RENAME	USER
REPAIR	REFRESH	TABLE
REPLACE	REPLACE	TABLE
REPLACE_SELECT	REPLACE	TABLE
RESET	RESET	TRACE
RESIGNAL	NOTIFY	SIGNAL
REVOKE	REVOKE	PRIVILEGE
REVOKE_ALL	REVOKE	PRIVILEGE
ROLLBACK	ROLLBACK	TRANSACTION
ROLLBACK_TO_SAVEPOINT	ROLLBACK	SAVEPOINT
SAVEPOINT	SET	SAVEPOINT
SELECT	SELECT	TABLE
SET_OPTION	SET	VARIABLE
SIGNAL	NOTIFY	SIGNAL
SHOW_BINLOG_EVENTS	RETRIEVE	EVENT
SHOW_BINLOGS	RETRIEVE	TRACE
SHOW_CHARSETS	RETRIEVE	PROPERTY
SHOW_COLLATIONS	RETRIEVE	PROPERTY
SHOW_CREATE_DB	RETRIEVE	STATEMENT
SHOW_CREATE_EVENT	RETRIEVE	STATEMENT
SHOW_CREATE_FUNC	RETRIEVE	STATEMENT
SHOW_CREATE_PROC	RETRIEVE	STATEMENT
SHOW_CREATE_TABLE	RETRIEVE	STATEMENT
SHOW_CREATE_TRIGGER	RETRIEVE	STATEMENT
SHOW_DATABASES	RETRIEVE	DATABASE

Table K-1 (Cont.) MySQL Audit Events

Source Event	Command Class	Target Type
SHOW_ENGINE_LOGS	RETRIEVE	TRACE
SHOW_ENGINE_MUTEX	RETRIEVE	MUTEX
SHOW_ENGINE_STATUS	RETRIEVE	STATUS
SHOW_EVENTS	RETRIEVE	DATABASE
SHOW_ERRORS	RETRIEVE	ERROR
SHOW_FIELDS	DESCRIBE	TABLE
SHOW_FUNCTION_CODE	RETRIEVE	FUNCTION
SHOW_FUNCTION_STATUS	RETRIEVE	STATUS
SHOW_GRANTS	RETRIEVE	USER
SHOW_KEYS	RETRIEVE	TABLE
SHOW_MASTER_STATUS	RETRIEVE	STATUS
SHOW_OPEN_TABLES	RETRIEVE	DATABASE
SHOW_PLUGINS	RETRIEVE	PLUGIN
SHOW_PRIVILEGES	RETRIEVE	PRIVILEGE
SHOW_PROCEDURE_CODE	RETRIEVE	PROCEDURE
SHOW_PROCEDURE_STATUS	RETRIEVE	STATUS
SHOW_PROCESSLIST	RETRIEVE	PROCESS
SHOW_PROFILE	RETRIEVE	QUERY
SHOW_PROFILES	RETRIEVE	PROFILE
SHOW_RELAYLOG_EVENTS	RETRIEVE	EVENT
SHOW_REPLICA_HOSTS	RETRIEVE	REPLICA
SHOW_REPLICA_STATUS	RETRIEVE	STATUS
SHOW_STATUS	RETRIEVE	STATUS
SHOW_STORAGE_ENGINES	RETRIEVE	PROPERTY
SHOW_TABLE_STATUS	RETRIEVE	DATABASE
SHOW_TABLES	RETRIEVE	DATABASE
SHOW_TRIGGERS	RETRIEVE	DATABASE
SHOW_VARIABLES	RETRIEVE	VARIABLE
SHOW_WARNINGS	RETRIEVE	WARNING
SHOW_CREATE_USER	RETRIEVE	STATEMENT
REPLICA_START	START	SYSTEM
REPLICA_STOP	STOP	SYSTEM
GROUP_REPLICATION_START	START	REPLICATION
GROUP_REPLICATION_STOP	STOP	REPLICATION
STMT_EXECUTE	EXECUTE	STATEMENT
STMT_CLOSE	CLOSE	STATEMENT

Table K-1 (Cont.) MySQL Audit Events

Source Event	Command Class	Target Type
STMT_FETCH	GET	STATEMENT
STMT_PREPARE	INITIALIZE	STATEMENT
STMT_RESET	RESET	STATEMENT
STMT_SEND_LONG_DATA	SEND	STATEMENT
TRUNCATE	TRUNCATE	TABLE
UNINSTALL_PLUGIN	UNINSTALL	PLUGIN
UNLOCK_TABLES	UNLOCK	TABLE
UPDATE	UPDATE	TABLE
UPDATE_MULTI	UPDATE	TABLE
XA_COMMIT	COMMIT	XA
XA_END	STOP	XA
XA_PREPARE	INITIALIZE	XA
XA_RECOVER	RECOVER	XA
XA_ROLLBACK	ROLLBACK	XA
XA_START	START	XA

L

Solaris Operating System Audit Events

Solaris operating system audit events can include events such as AUE_AT_CREATE and AUE_AT_DELETE.

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 Audit Vault and Database Firewall 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 for Oracle Audit Vault and Database Firewall data warehouse details that may be useful in designing your own reports.

Table L-1 lists the Solaris audit events and the equivalent Oracle Audit Vault and Database Firewall events.

Table L-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

Table L-1 (Cont.) Solaris Audit Events

Source Event	Command Class	Target Type
AUE_DA_LIST_DEVICES	LIST	DEVICE
AUE_DETACH	UNMOUNT	DEVICE
AUE_REMOVE	EJECT	DEVICE
AUE_SMSERVERD	CONTROL	DEVICE
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

Table L-1 (Cont.) Solaris Audit Events

Source Event	Command Class	Target Type
AUE_EXEC	EXECUTE	FILE
AUE_EXECVE	EXECUTE	FILE
AUE_FACCESSAT	CHECK	FILE
AUE_FACLSET	SET	FILE
AUE_FCHMOD	SET	FILE
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

Table L-1 (Cont.) Solaris Audit Events

Source Event	Command Class	Target Type
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
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

Table L-1 (Cont.) Solaris Audit Events

Source Event	Command Class	Target Type
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
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

Table L-1 (Cont.) Solaris Audit Events

Source Event	Command Class	Target Type
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
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

Table L-1 (Cont.) Solaris Audit Events

Source Event	Command Class	Target Type
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
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

Table L-1   (Cont.) Solaris Audit Events

Source Event	Command Class	Target Type
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
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

Table L-1 (Cont.) Solaris Audit Events

Source Event	Command Class	Target Type
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
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

Table L-1 (Cont.) Solaris Audit Events

Source Event	Command Class	Target Type
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
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

Table L-1 (Cont.) Solaris Audit Events

Source Event	Command Class	Target Type
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
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	None
AUE_INIT_SOLARIS	SET	None

Table L-1 (Cont.) Solaris Audit Events

Source Event	Command Class	Target Type
AUE_POWEROFF_SOLARIS	SHUTDOWN	None
AUE_REBOOT_SOLARIS	REBOOT	None
AUE_SHUTDOWN_SOLARIS	SHUTDOWN	None
AUE_UADMIN_DUMP	DUMP	None
AUE_UADMIN_FREEZE	SUSPEND	None
AUE_UADMIN_FTRACE	TRACE	None
AUE_UADMIN_REBOOT	REBOOT	None
AUE_UADMIN_SHUTDOWN	SHUTDOWN	None
AUE_UADMIN_THAW	RESUME	None

M

Microsoft Windows Operating System Audit Events

Microsoft Windows Operating System audit events capture events such as ACCOUNT_FAILED_TO_LOGON and ACL_SET_ON_ACCOUNT.

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 Audit Vault and Database Firewall 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 for Oracle Audit Vault and Database Firewall data warehouse details that may be useful in designing your own reports.

Table M-1 lists the Windows audit events and the equivalent Oracle Audit Vault and Database Firewall events.

Table M-1 Windows Audit Events

Source Event	Command Class	Target Type
ACCOUNT_LOGON_SUCCESSFUL	LOGIN	ACCOUNT
ACL_SET_ON_ACCOUNT	SET	ACCOUNT
ACCOUNT_COULD_NOT_MAP_FOR_LOGON	LOGIN	ACCOUNT
ACCOUNT_FAILED_TO_LOGON	LOGIN	ACCOUNT
ACCOUNT_MAPPED_FOR_LOGON	LOGIN	ACCOUNT
ASSIGNED_PRIMARY_TOKEN_TO_PROCESS	ASSIGN	PROCESS
ATTEMPT_MADE_TO_REGISTER_SECURITY_EVENT_SOURCE	REGISTER	LOG
ATTEMPT_MADE_TO_UNREGISTER_SECURITY_EVENT_SOURCE	UNREGISTER	LOG
ATTEMPT_TO_ADD_SID_HISTORY_TO_ACCOUNT_FAILED	INSERT	ACCOUNT
ATTEMPT_TO_QUERY_EXISTANCE_OF_BLANK_PASSWORD_FOR_ACCOUNT	ANALYZE	ACCOUNT
ATTEMPTED_TO_MODIFY_ACCOUNT_PASSWORD	UPDATE	ACCOUNT
ATTEMPTED_TO_RESET_ACCOUNT_PASSWORD	RESET	ACCOUNT
ATTEMPTED_TO_VALIDATE_ACCOUNT_CREDENTIAL	VALIDATE	ACCOUNT
AUDIT_FILTER_FOR_CERTIFICATE_SERVICE_CHANGED	UPDATE	SERVICE
BACKED_UP_CREDENTIAL_MANAGER_CREDENTIALS	BACKUP	MANAGER

Table M-1 (Cont.) Windows Audit Events

Source Event	Command Class	Target Type
BASIC_APPLICATION_GROUP_CREATED	CREATE	GROUP
BASIC_APPLICATION_GROUP_DELETED	DELETE	GROUP
BASIC_APPLICATION_GROUP_MODIFIED	UPDATE	GROUP
CENTRAL_ACCESS_POLICIES_ON_THE_MACHINE_HAVE_BEEN_CHANGED	UPDATE	POLICY
CENTRAL_ACCESS_POLICY_ON_THE_OBJECT_CHANGED	UPDATE	OBJECT
CERTIFICATE_MANAGER_SETTINGS_FOR_CERTIFICATE_SERVICE_MODIFIED	UPDATE	SERVICE
CERTIFICATE_REQUEST_ATTRIBUTES_MODIFIED	UPDATE	CERTIFICATE
CERTIFICATE_REQUEST_EXTENSION_MODIFIED	UPDATE	CERTIFICATE
CERTIFICATE_SERVICES_PUBLISHED_CRL	PUBLISH	CRL
CERTIFICATE_SERVICE_APPROVED_CERTIFICATE_REQUEST_AND_ISSUED_CERTIFICATE	GRANT	SERVICE
CERTIFICATE_SERVICE_ARCHIVED_KEY	ARCHIVE	SERVICE
CERTIFICATE_SERVICE_BACKUP_COMPLETED	BACKUP	SERVICE
CERTIFICATE_SERVICE_BACKUP_STARTED	BACKUP	SERVICE
CERTIFICATE_SERVICE_CONFIGURATION_ENTRY_MODIFIED	UPDATE	SERVICE
CERTIFICATE_SERVICE_DENIED_CERTIFICATE_REQUEST	DENY	SERVICE
CERTIFICATE_SERVICE_IMPORTED_AND_ARCHIVED_KEY	ARCHIVE	SERVICE
CERTIFICATE_SERVICE_IMPORTED_CERTIFICATE_IN_ITS_DATABASE	IMPORT	SERVICE
CERTIFICATE_SERVICE_LOADED_TEMPLATE	LOAD	TEMPLATE
CERTIFICATE_SERVICE_PROPERTY_MODIFIED	UPDATE	SERVICE
CERTIFICATE_SERVICE_RETRIEVED_ARCHIVED_KEY	RETRIEVE	SERVICE
CERTIFICATE_SERVICE_RECEIVED_CERTIFICATE_REQUEST	RECEIVE	SERVICE
CERTIFICATE_SERVICE_RECEIVED_SHUT_DOWN_REQUEST	RECEIVE	SERVICE
CERTIFICATE_SERVICE_RESTORE_STARTED	RESTORE	SERVICE
CERTIFICATE_SERVICE_RESTORE_COMPLETED	RESTORE	SERVICE
CERTIFICATE_SERVICE_SECURITY_PERMISSIONS_MODIFIED	UPDATE	SERVICE
CERTIFICATE_SERVICE_SET_CERTIFICATE_REQUEST_STATUS_TO_PENDING	SET	SERVICE
CERTIFICATE_SERVICE_STARTED	START	SERVICE
CERTIFICATE_SERVICE_STOPPED	STOP	SERVICE
CERTIFICATE_SERVICE_PUBLISHED_CA_CERTIFICATE_TO_ACTIVE_DIRECTORY_DOMAIN_SERVICES	PUBLISH	SERVICE
CERTIFICATE_SERVICES_RECEIVED_RESUBMITTED_CERTIFICATE_REQUEST	RECEIVE	CERTIFICATE
CERTIFICATE_SERVICES_RECEIVED_CERTIFICATE_REVOKATION_LIST_PUBLISH_REQUEST	RECEIVE	CRL
CERTIFICATE_SERVICES_REVOKED_CERTIFICATE	REVOKE	CERTIFICATE
COMPUTER_ACCOUNT_CREATED	CREATE	ACCOUNT

Table M-1 (Cont.) Windows Audit Events

Source Event	Command Class	Target Type
COMPUTER_ACCOUNT_DELETED	DELETE	ACCOUNT
COMPUTER_ACCOUNT_MODIFIED	UPDATE	ACCOUNT
CHANGED_TYPE_OR_SCOPE_OF_GROUP	UPDATE	GROUP
CREATED_USER_ACCOUNT	CREATE	ACCOUNT
CREATED_NEW_PROCESS	START	PROCESS
DISABLED_USER_ACCOUNT	DISABLE	ACCOUNT
DELETED_USER_ACCOUNT	DELETE	ACCOUNT
ENABLED_USER_ACCOUNT	ENABLE	ACCOUNT
EXITED_PROCESS	STOP	PROCESS
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
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
LDAP_QUERY_GROUP_CREATED	CREATE	GROUP
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

Table M-1 (Cont.) Windows Audit Events

Source Event	Command Class	Target Type
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
MODIFIED_USER_ACCOUNT	UPDATE	ACCOUNT
LOCKED_OUT_USER_ACCOUNT	LOCK	ACCOUNT
SID_HISTORY_ADDED_TO_ACCOUNT	UPDATE	ACCOUNT
UNLOCKED_USER_ACCOUNT	UNLOCK	ACCOUNT
MODIFIED_ACCOUNT_NAME	UPDATE	ACCOUNT
MODIFIED_DIRECTORY_SERVICE_RESTORE_MODE_ADMIN_PASSWORD	UPDATE	SERVICE
RESTORED_CREDENTIAL_MANAGER_CREDENTIALS	RESTORE	MANAGER
REMOTE_PROCEDURE_CALL_ATTEMPTED	REMOTE CALL	PROCEDURE
LOGGED_OFF_ACCOUNT	LOGOUT	ACCOUNT
USER_INITIATED_LOGOFF	LOGOUT	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

Table M-1 (Cont.) Windows Audit Events

Source Event	Command Class	Target Type
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
INVOKED_SCREEN_SAVER	CALL	SCREEN SAVER
DISMISSED_SCREEN_SAVER	ABORT RELEASE	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
ROWS_DELETED_FROM_CERTIFICATE_DATABASE	DELETE	DATABASE
ENABLED_ROLE_SEPERATION_ON_CERTIFICATION_AUTHORITY	ENABLE	ROLE
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

Table M-1 (Cont.) Windows Audit Events

Source Event	Command Class	Target Type
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
CRASHONAUDITFAIL_VALUE_MODIFIED	UPDATE	CRASHONAUDIT FAIL
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	PRIVILEGE
USER_RIGHT_REMOVED	DROP	PRIVILEGE
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

Table M-1   (Cont.) Windows Audit Events

Source Event	Command Class	Target Type
SE_AUDITID_ETW_IPSEC_POLICY_FAILURE	EXECUTE	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
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

Table M-1 (Cont.) Windows Audit Events

Source Event	Command Class	Target Type
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	GET	INTERFACE
SE_AUDITID_ETW_POLICYAGENT_IPSECSVC_RPC_INIT_FAILURE	INITIALIZE	SERVICE
SE_AUDITID_ETW_POLICYAGENT_IPSECSVC_ERROR_SHUTDOWN	STOPE	SERVICE
SE_AUDITID_ETW_POLICYAGENT_IPSECSVC_FAILED_PNP_FILTER_PROCESSING	EXECUTE	FILTER
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	READ	POLICY
SE_AUDITID_ETW_MPSFIREWALL_INIT_DRIVER_FAILURE	INITIALIZE	DRIVER
SE_AUDITID_ETW_MPSFIREWALL_SERVICE_STARTUP_FAILURE	START	SERVICE
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	START	DRIVER
SE_AUDITID_ETW_MPSFIREWALL_DRIVER_CRITICAL_ERROR	STOP	DRIVER
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
CRYPTOGRAPHIC_PRIMITIVE_OPERATION_FAILED	EXECUTE	OPERATION
VERIFICATION_OPERATION_FAILED	VALIDATE	OPERATION

Table M-1 (Cont.) Windows Audit Events

Source Event	Command Class	Target Type
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
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
USER_DEVICE_CLAIMS_INFORMATION	LOGIN	ACCOUNT
PROPOSED_CENTRAL_ACCESS_POLICY_DOES_NOT_GRANT_SAME_ACCESS_PERMISSIONS_AS_CURRENT	UPDATE	POLICY
RESOURCE_ATTRIBUTES_OF_THE_OBJECT_CHANGED	UPDATE	POLICY
KEY_ACCESS_DENIED_BY_MICROSOFT_KEY_DISTRIBUTION_SERVICE	DENY	SERVICE
WINDOWS_FILTERING_PLATFORM_BLOCKED_PACKET	BLOCK	PACKET
RESTRICTIVE_WINDOWS_FILTERING_PLATFORM_BLOCKED_PACKET	BLOCK	PACKET
SERVICE_CONNECTION_POINT_OBJECT_COULD_NOT_BE_PARSED	READ	OBJECT
KERBEROS_TICKET_GRANTING_TICKIT_DENIED	DENY	SYSTEM
KERBEROS_SERVICE_TICKET_DENIED	DENY	SYSTEM
NTLM_AUTHETICATION_FAILED	AUTHENTICATE	ACCOUNT
KERBEROS_PREAUTHETICATION_FAILED	AUTHENTICATE	ACCOUNT
GROUP_MEMBERSHIP_INFORMATION	LOGIN	GROUP
SECURITY_GROUP_ENUMERATED	CALCULATE	GROUP

Table M-1 (Cont.) Windows Audit Events

Source Event	Command Class	Target Type
USER_LOCAL_GROUP_ENUMERATED	CALCULATE	GROUP
BOOT_CONFIGURATION_DATA_LOADED	LOAD	CONFIGURATION
INTEGRITY_CHECK_TO_LOAD_INTO_PROCESS_FAILED_FOR_FILE	LOAD	FILE
EXTERNAL_DEVICE_RECOGNIZED	CONNECT	DEVICE
DEVICE_DISABLE_REQUESTED	REQUEST	DEVICE
DEVICE_DISABLED	DISABLE	DEVICE
DEVICE_ENABLE_REQUESTED	REQUEST	DEVICE
DEVICE_ENABLED	ENABLE	DEVICE
DEVICE_INSTALLATION_FORBIDDED	INSTALL	DEVICE
FORBIDDEN_DEVICE_INSTALLATION_ALLOWED	INSTALL	DEVICE
FIPS_MODE_SELFTESTS_SUCCEEDED	VALIDATE	PROCESS
FIPS_MODE_SELFTESTS_FAILED	VALIDATE	PROCESS
USER_RIGHT_ADJUSTED	UPDATE	PRIVILEGE

N

Linux Operating System Audit Events

Linux operation system events include events such as LOGIN, USER_AUTH, and USER_ACCT.

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 Audit Vault and Database Firewall 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 for Oracle Audit Vault and Database Firewall data warehouse details that may be useful in designing your own reports.

Table N-1 lists the Linux audit events and the equivalent Oracle Audit Vault and Database Firewall events.

Table N-1 Linux Audit Events

Source Event	Additional Description	Command Class	Target Type
LOGIN	None	LOGON	SYSTEM
USER_AUTH	None	AUTHENTICATE	USER
USER_ACCT	None	AUTHORIZE	USER
CRED_ACQ	None	ACQUIRE	USER
CRED_DISP	None	RESET	USER
DAEMON_START	None	AUDIT	AUDITSERVICE
DAEMON_END	None	NOAUDIT	AUDITSERVICE
DAEMON_ABORT	None	NOAUDIT	AUDITSERVICE
DAEMON_CONFIG	None	CONFIGURE	AUDITSERVICE
DAEMON_ROTATE	None	UPDATE	AUDITSERVICE
DAEMON_RESUME	None	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

Table N-1 (Cont.) Linux Audit Events

Source Event	Additional Description	Command Class	Target Type
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	None	START	SESSION
AVC	None	ACCESS	PRIVILEGE
MAC_POLICY_LOAD	None	ENABLE	POLICY
MAC_STATUS	None	UPDATE	SYSTEM
MAC_CONFIG_CHANGE	None	MODIFY	RULE
MAC_UNLBL_ALLOW	None	UPDATE	MODULE
MAC_CIPSOV4_ADD	None	CREATE	MODULE
MAC_CIPSOV4_DEL	None	DELETE	USER
MAC_MAP_ADD	None	CREATE	MODULE
MAC_MAP_DEL	None	DELETE	MODULE
MAC_IPSEC_ADDSA	None	CREATE	MODULE
MAC_IPSEC_DELSA	None	DELETE	MODULE
MAC_IPSEC_ADDSPD	None	MODIFY	MODULE
MAC_IPSEC_DELSPD	None	DELETE	MODULE
ANOM_PROMISCUOUS	None	UPDATE	DEVICE
ANOM_ABEND	None	EXECUTE	MODULE
ANOM_LOGIN_FAILURES	None	LOGIN	USER
ANOM_LOGIN_TIME	None	LOGIN	USER
ANOM_LOGIN_SESSIONS	None	LOGIN	USER
ANOM_LOGIN_LOCATION	None	LOGON	USER
RESP_ACCT_UNLOCK_TIMED	None	ENABLE	USER
RESP_ACCT_LOCK	None	LOCK	USER
TTY	None	EXECUTE	KEYSTROKE
USER_AVC	None	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

Table N-1 (Cont.) Linux Audit Events

Source Event	Additional Description	Command Class	Target Type
LABEL_OVERRIDE	None	UPDATE	OBJECT
LABEL_LEVEL_CHANGE	None	UPDATE	OBJECT
USER_LABELED_EXPORT	None	EXPORT	OBJECT
USER_UNLABELED_EXPORT	None	EXPORT	OBJECT
USER_START	None	START	USER
USER_END	None	END	USER
CRED_REFR	None	REFRESH	USER
USER_LOGIN	None	LOGIN	ACCOUNT
USER_LOGOUT	None	LOGOUT	ACCOUNT
USER_ERR	None	RAISE	USER
USYS_CONFIG	None	UPDATE	USER
USER_CMD	None	EXECUTE	PROGRAM
FS_RELABEL	None	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

Table N-1 (Cont.) Linux Audit Events

Source Event	Additional Description	Command Class	Target Type
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
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

Table N-1 (Cont.) Linux Audit Events

Source Event	Additional Description	Command Class	Target Type
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
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	None	UPDATE	USER
USER_TTY	None	EXECUTE	KEYSTROKE
ADD_GROUP	None	ADD	GROUP
ADD_USER	None	CREATE	USER
DEL_USER	None	DELETE	USER
SYSCALL	None	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

Table N-1 (Cont.) Linux Audit Events

Source Event	Additional Description	Command Class	Target Type
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
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

Table N-1 (Cont.) Linux Audit Events

Source Event	Additional Description	Command Class	Target Type
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
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

Table N-1 (Cont.) Linux Audit Events

Source Event	Additional Description	Command Class	Target Type
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
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

Table N-1 (Cont.) Linux Audit Events

Source Event	Additional Description	Command Class	Target Type
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
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

Table N-1 (Cont.) Linux Audit Events

Source Event	Additional Description	Command Class	Target Type
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
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

Table N-1 (Cont.) Linux Audit Events

Source Event	Additional Description	Command Class	Target Type
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
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

Table N-1 (Cont.) Linux Audit Events

Source Event	Additional Description	Command Class	Target Type
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
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

Table N-1 (Cont.) Linux Audit Events

Source Event	Additional Description	Command Class	Target Type
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
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	None	RAISE	SYSTEM
SYSTEM_SHUTDOWN	None	SHUTDOWN	OS
ROLE_REMOVE	None	DELETE	ROLE
ROLE_ASSIGN	None	ASSIGN	ROLE
SYSTEM_RUNLEVEL	None	STOP	SYSTEM
NETFILTER_CFG	None	CONFIGURE	SOCKET
DEL_GROUP	None	DELETE	GROUP
CRYPTO_KEY_USER	None	DISCONNECT	USER SESSION
USER_MGMT	User account attribute change	UPDATE	USER

Table N-1 (Cont.) Linux Audit Events

Source Event	Additional Description	Command Class	Target Type
DAC_CHECK	User space DAC check results	VALIDATE	PRIVILEGE
DAEMON_RECONFIG	Auditd should be reconfigured	CONFIGURE	AUDITSERVICE
ANOM_MOD_ACCT	Changing an account	UPDATE	ACCOUNT
RESP_EXEC	Execute a script	EXECUTE	SCRIPT
USER_MAC_POLICY_LOAD	User’s PC daemon loaded policy	LOAD	POLICY
USER_MAC_CONFIG_CHANGE	Change made to MAC policy	UPDATE	POLICY
ANOM_LINK	Suspicious use of file links	ACCESS	FILE
GRP_MGMT	Group account attribute was modified	UPDATE	GROUP
GRP_MGMT	Group is created	CREATE	GROUP
GRP_CHAUTHTOK	Group account password or pin changed	UPDATE	GROUP
ACCT_LOCK	User account locked by administrator	LOCK	USER
ACCT_UNLOCK	User account unlocked by administrator	UNLOCK	USER
DAEMON_ERR	Auditd daemon internal error is detected	ERROR	AUDITSERVICE
OBJ_PID	Records information about a process to which a signal is sent	SEND	PROCESS
PATH	Records information about file name path	EXECUTE	FILE
PROCTITLE	Provides the full command line that triggered this audit event. Triggered by system call to the kernel	EXECUTE	SYSCALL
AVC_PATH	Records the dentry and vfsmount pair when SE Linux permission check occurs	ACCESS	PRIVILEGE
MAC_CHECK	User space MAC decision is made	ACCESS	USER
SECCOMP	Triggered when a secure computing event is detected	FIND	EVENT
CRYPTO_IKE_SA	Internet Key Exchange Security Association establishment	START	SESSION
CRYPTO_IPSEC_SA	Internet Protocol Security Association establishment	START	SESSION
CAPSET	Records any changes in process based capabilities	UPDATE	PROCESS
CWD	Record the current working directory	GET	DIRECTORY
EOE	Records the end of a multi record event	EXECUTE	EVENT

Table N-1 (Cont.) Linux Audit Events

Source Event	Additional Description	Command Class	Target Type
EXECVE	Records arguments of the execve(2) system call	EXECUTE	SYSCALL
FD_PAIR	Records the use of the pipe and socket pair system calls	EXECUTE	SYSCALL
FEATURE_CHANGE	Audit feature value has been changed	UPDATE	AUDITSERVICE
IPC	Records information about an inter process communication object referenced by a system call	EXECUTE	SYSCALL
MMAP	Records a file descriptor and flags of the mmap(2) system call	EXECUTE	SYSCALL
MQ_GETSETATTR	Records the mq_getattr(3) and mq_setattr(3) message queue attributes	EXECUTE	SYSCALL
MQ_NOTIFY	Records arguments of the mq_notify(3) system call	EXECUTE	SYSCALL
MQ_OPEN	Records arguments of the mq_open(3) system call	EXECUTE	SYSCALL
MQ_SENDRECV	Records arguments of the mq_send(3) and mq_recieve(3) system calls	EXECUTE	SYSCALL
KERN_MODULE	Records a kernel module name on load or unload	EXECUTE	MODULE
SOCKADDR	Records socket address	EXECUTE	SOCKET
SOCKETCALL	Records arguments of the sys_socket call system call	EXECUTE	SYSCALL
TEST	Records the success value of a test message	VALIDATE	MESSAGE
TRUSTED_APP	The record of this type can be used by third party application that requires auditing	EXECUTE	AUDITSERVICE

O

Oracle ACFS Audit Events

Oracle ACFS audit events include events such as `ACFS_SEC_PREPARE` and `ACFS_SEC_REALM_CREATE`.

> **Note:**
>
> Oracle Automatic Storage Management Cluster File System (Oracle ACFS) or Oracle Advanced Cluster File System was deprecated in Oracle AVDF release 20.7 and is desupported in 20.8.

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 Audit Vault and Database Firewall 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 Audit Vault and Database Firewall).
- For file system objects `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 Audit Vault and Database Firewall).

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 for Oracle Audit Vault and Database Firewall data warehouse details that may be useful in designing your own reports.

Table O-1 lists the Oracle ACFS Security Objects audit events and the equivalent Oracle Audit Vault and Database Firewall events.

Table O-1 Oracle ACFS Security Objects Audit Events

Source Event	Command Class	Target Object	Associate Objects	Status
ACFS_SEC_PREPARE	ENABLE	Mount Point	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
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	Mount Point	None	SUCCESS
ACFS_SEC_LOAD	RESTORE	Mount Point	None	SUCCESS
ACFS_ENCR_SET	SET	Mount Point	AES-128/192/256	SUCCESS
ACFS_ENCR_VOL_REKEY	REKEY	Mount Point	AES-128/192/256	SUCCESS
ACFS_ENCR_FS_ON	ENABLE	MountPoint	Encryption	SUCCESS
ACFS_ENCR_FS_OFF	DISABLE	Mount Point	Encryption	SUCCESS
ACFS_ENCR_FILE_REKEY	REKEY	File name	AES-128/192/256	SUCCESS
ACFS_ENCR_FILE_ON	ENABLE	File name	None	SUCCESS
ACFS_ENCR_FILE_OFF	DISABLE	File name	None	SUCCESS
ACFS_AUDIT_ENABLE	ENABLE	Mount Point	Audit	SUCCESS
ACFS_AUDIT_DISABLE	DISABLE	Mount Point	Audit	SUCCESS
ACFS_AUDIT_PURGE	PURGE	Mount Point	Audit trail	SUCCESS
ACFS_AUDIT_AUTO_PURGE	PURGE	Mount Point	Audit trail	SUCCESS
ACFS_AUDIT_READ	READ	Mount Point	Audit trail	SUCCESS
ACFS_AUDIT_ARCHIVE	ARCHIVE	Acfsutil command	None	SUCCESS
ACFS_AUDIT_SIZE	AUDIT	Acfsutil command	None	SUCCESS

Table O-1   (Cont.) Oracle ACFS Security Objects Audit Events

Source Event	Command Class	Target Object	Associate Objects	Status
ACFS_AUDIT_FAILURE	AUDIT	Acfsutil command	None	FAILURE
ACFS_SEC_ADMIN_PRIV	AUTHORIZE	Acfsutil command	None	FAILURE
ACFS_SEC_ADMIN_AUTH_FAIL	AUTHORIZE	Acfsutil command	None	FAILURE
ACFS_SYS_ADMIN_PRIV	AUTHORIZE	Acfsutil command	None	FAILURE
ACFS_AUDIT_MGR_PRIV	AUTHORIZE	Acfsutil command	None	FAILURE
ACFS_AUDITOR_PRIV	AUTHORIZE	Acfsutil command	None	FAILURE
ACFS_INSUFFICIENT_PRIV	AUTHORIZE	Acfsutil command	None	FAILURE
ACFS_ENCR_WALLET_AUTH_FAIL	AUTHORIZE	Acfsutil command	None	FAILURE
ACFS_SEC_CMD_FAIL	AUTHORIZE	Acfsutil command	None	FAILURE

Table O-2 lists the Oracle ACFS File System Objects audit events and the equivalent Oracle Audit Vault and Database Firewall events.

Table O-2   Oracle ACFS File System Objects Audit Events

Source Event	Command Class	Target Object	Associate Objects	Status

ACFS_AUDIT_READ_OP	READ	File name	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE
				ACFS_REALM_AUTH = SUCCESS

ACFS_AUDIT_WRITE_OP	WRITE	File name	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE
				ACFS_REALM_AUTH = SUCCESS

ACFS_AUDIT_DELETE_OP	DELETE	File name	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE
				ACFS_REALM_AUTH = SUCCESS

ACFS_AUDIT_OPEN_OP	OPEN	File name	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE
				ACFS_REALM_AUTH = SUCCESS

ACFS_AUDIT_RENAME_OP	RENAME	File name	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE
				ACFS_REALM_AUTH = SUCCESS

ACFS_AUDIT_CREATEFILE_OP	CREATE	File name	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE
				ACFS_REALM_AUTH = SUCCESS

Table O-2 (Cont.) Oracle ACFS File System Objects Audit Events

Source Event	Command Class	Target Object	Associate Objects	Status

ACFS_AUDIT_MAKEDIR_OP	CREATE	Directory name	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE
				ACFS_REALM_AUTH = SUCCESS

ACFS_AUDIT_READDIR_OP	READ	Directory name	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE
				ACFS_REALM_AUTH = SUCCESS

ACFS_AUDIT_OVERWRITE_OP	WRITE	File name	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE
				ACFS_REALM_AUTH = SUCCESS

ACFS_AUDIT_TRUNCATE_OP	TRUNCATE	File name	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE
				ACFS_REALM_AUTH = SUCCESS

ACFS_AUDIT_MMAPREAD_OP	READ	File name	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE
				ACFS_REALM_AUTH = SUCCESS

ACFS_AUDIT_MMAPWRITE_OP	WRITE	File name	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE
				ACFS_REALM_AUTH = SUCCESS

ACFS_AUDIT_EXTEND_OP	WRITE	File name	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE
				ACFS_REALM_AUTH = SUCCESS

ACFS_AUDIT_CHOWN_OP	CHOWN	File name/Directory name	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE
				ACFS_REALM_AUTH = SUCCESS

ACFS_AUDIT_CHGRP_OP	CHGRP	File name/Directory name	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE
				ACFS_REALM_AUTH = SUCCESS

ACFS_AUDIT_CHMOD_OP	CHMOD	File name/Directory name	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE
				ACFS_REALM_AUTH = SUCCESS

ACFS_AUDIT_SYMLINK_OP	SYMLINK	File name/Directory name	Realms and command rules	ACFS_REALM_VIOLATION = FAILURE
				ACFS_REALM_AUTH = SUCCESS

Table O-2 (Cont.) Oracle ACFS File System Objects Audit Events

Source Event	Command Class	Target Object	Associate Objects	Status

`ACFS_AUDIT_LINKFILE_OP`	`LINK`	File name/Directory name	Realms and command rules	`ACFS_REALM_VIOLATION = FAILURE`
				`ACFS_REALM_AUTH = SUCCESS`

Related Topics

- Behavior Changes, Deprecation, and Desupport Notices in Oracle Audit Vault and Database Firewall 20.7

P

Active Directory Audit Events

Learn about Active Directory audit events.

P.1 About Active Directory Audit Events

The Active Directory audit events are categorized by Directory Service audit trail events and Security audit trail 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 Audit Vault and Database Firewall 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 for Oracle Audit Vault and Database Firewall data warehouse details that may be useful in designing your own reports.

P.2 Directory Service Audit Trail Events

Directory Service audit trail events include events such as DATABSE_STOPPED_WITH_ERROR and DATABASE_STARTED.

Table P-1 lists the Directory Service audit trail events and their **command_class** and **target_type** mappings in the Oracle AVDF audit record.

Table P-1 Directory Service Audit Trail Events

Event ID	Source Event	Command Class	Target Type
104	DATABSE_STOPPED_WITH_ERROR	STOP	INSTANCE
105	DATABASE_STARTED	START	INSTANCE
106	PARAMETER_UPDATE_OVERRIDDEN	SET	OBJECT
107	PARAMETER_READ_REJECTED	READ	OBJECT
108	ESE_CONFIGURATION_STORE_LOCKED	LOCK	CONFIGURATION
203	STOPPED_DATABASE_BACKUP_WITH_ERROR	BACKUP	DATABASE
214	DATABASE_BACKUP_STOPPED_WITH_ERROR	BACKUP	DATABASE
217	ERROR_DURING_DATABASE_FILE_BACKUP	BACKUP	FILE
328	CALLBACK_FOR_ATTACH_OF_DATABASE	EXECUTE	CALLBACK
329	CALLBACK_FOR_DETACH_OF_DATABSE	RECOVER	DATABASE

Table P-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	DATBSE_RECOVERY_FAILED	RECOVER	DATABASE
516	DATABASE_VERIFICATION_FAILED	VALIDATE	DATABASE
633	DATABASE_RECOVERY_PAUSED	PAUSE	DATABASE
634	DATABASE_RECOVERY_PAUSED_LONGER	PAUSE	DATABASE
705	ONLINE_DEFRAGMENTATION_OF_DATABASE_TERMINATED_PREMATURELY	END	DEFRAGMENTATION
916	BETA_FEATURE_ENABLED	ENABLE	FEATURE
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
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

Table P-1 (Cont.) Directory Service Audit Trail Events

Event ID	Source Event	Command Class	Target Type
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
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

Table P-1 (Cont.) Directory Service Audit Trail Events

Event ID	Source Event	Command Class	Target Type
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	END	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
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

Table P-1 (Cont.) Directory Service Audit Trail Events

Event ID	Source Event	Command Class	Target Type
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
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

Table P-1 (Cont.) Directory Service Audit Trail Events

Event ID	Source Event	Command Class	Target Type
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
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

Table P-1 (Cont.) Directory Service Audit Trail Events

Event ID	Source Event	Command Class	Target Type
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
1561	DIRLOG_DRA_USER_REQ_FULL_SYNC	SYNCHRONIZE	PARTITION
1562	DIRLOG_DRA_FULL_SYNC_CONTINUED	SYNCHRONIZE	PARTITION

Table P-1 (Cont.) Directory Service Audit Trail Events

Event ID	Source Event	Command Class	Target Type
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 P-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

Table P-1 (Cont.) Directory Service Audit Trail Events

Event ID	Source Event	Command Class	Target Type
1921	BACKUP_RESTORE_FAILED_WHILE_AD_DS_READ_OPERATION	BACKUP	DOMAIN SERVICE
1923	CONVERT_COMPUTER_ACCOUNT_TO_ADDC_ACCOUNT	CONVERT	ACCOUNT
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

Table P-1 (Cont.) Directory Service Audit Trail Events

Event ID	Source Event	Command Class	Target Type
2027	CREATE_APPLICATION_DIRECTORY_PARTITION_FAILED_INSUFFICIENT_PERMISSION	CREATE	PARTITION
2029	CERTIFICATE_AUTHENTICATION_FAILED	AUTHENTICATE	CERTIFICATE
2032	AD_DS_BACKUP_PREPARATION_FAILED	INITIALIZE	BACKUP
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
2057	FAILED_TO_DELETE_REGISTRY_KEY	DROP	REGISTRY
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
2099	ATTRIBUTE_VALUE_CHANGE_APPLIED	UPDATE	ATTRIBUTE
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
2121	DISABLE_RECYCLEBIN	DISABLE	RECYCLEBIN
2184	EXCEEDED_NO_OF_DC_ACCOUNTS_LIMIT	EXCEED	ACCOUNT
2185	STOP_FRS_DFSR_SERVICE	STOP	SERVICE
2186	FAILED_TO_STOP_FRS_DFSR_SERVICE	STOP	SERVICE
2187	START_FRS_DFSR_SERVICE	START	SERVICE
2188	FAILED_TO_START_FRS_DFSR_SERVICE	START	SERVICE
2190	SET_REGISTRY_TO_INIT_SYSVOL_REPLICA	SET	REGISTRY
2191	SET_REGISTRY_TO_DISABLE_DNS_UPDATE	SET	REGISTRY
2192	FAILED_TO_SET_REGISTRY_TO_DISABLE_DNS_UPDATE	SET	REGISTRY
2193	SET_REGISTRY_TO_ENABLE_DNS_UPDATE	SET	REGISTRY
2194	FAILED_TO_SET_REGISTRY_TO_ENABLE_DNS_UPDATE	SET	REGISTRY
2196	FAILED_TO_ENABLE_SHUTDOWN_PRIVILEGE	ENABLE	PRIVILEGE
2197	FAILED_TO_INITIALIZE_SYSTEM_SHUTDOWN	INITIALIZE	SHUTDOWN

Table P-1 (Cont.) Directory Service Audit Trail Events

Event ID	Source Event	Command Class	Target Type
2208	DELETE_DFSR_DATABASE_TO_INIT_SYSVOL_REPLICA	DROP	DATABASE
2209	FAILED_TO_DELETE_DFSR_DATABASE	DROP	DATABASE
2210	FAILED_TO_CREATE_OBJECTS_FOR_CLONED_DC	CREATE	OBJECT
2221	FAILED_TO_GENERATE_RANDOM_PWD_FOR_CLONED_DC	CREATE	PASSWORD
2222	FAILED_TO_SET_PWD_FOR_CLONED_DC	SET	PASSWORD
2223	SET_MACHINE_ACCOUNT_PWD_FOR_CLONED_DC	SET	PASSWORD
2224	FAILED_TO_CLONE_VIRTUAL_DC	COPY	DOMAIN CONTROLLER
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
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

Table P-1 (Cont.) Directory Service Audit Trail Events

Event ID	Source Event	Command Class	Target Type
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
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

Table P-1 (Cont.) Directory Service Audit Trail Events

Event ID	Source Event	Command Class	Target Type
2866	ABORT_OBJECT_OPERATION_AS_LOGGING_MAX_LIMIT_REACHED	END	OPERATION
2869	CANT_START_INSTALL_FROM_MEDIA_PROMOTION_OF_DOMAINCONTROLLER	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
2898	EXCEED_NO_OF_RESULT_SET_PER_CONNECTION_LIMIT	EXCEED	RESULTSET
2899	EXCEED_MAX_RESULT_SET_SIZE_LIMIT	EXCEED	RESULTSET
2900	DETECTED_DIFFERENT_SEARCH_ARGUMENT	UPDATE	SEARCH
2905	INCOMPATIBLE_FUNCTIONAL_LEVEL_OF_DOMAIN_WITH_OS	COMPARE	LEVEL
2907	EXCEED_NO_OF_ADDS_DB_SESSIONS_LIMIT	EXCEED	SESSION
2908	INCOMPATIBLE_FUNCTIONAL_LEVEL_OF_DOMAIN_WITH_LOCAL_ADDC	COMPARE	LEVEL
2911	INCOMPATIBLE_DOMAIN_FUNCTIONAL_LEVEL_WITH_OS	COMPARE	LEVEL
2912	INCOMPATIBLE_FOREST_FUNCTIONAL_LEVEL_WITH_OS	COMPARE	LEVEL
2913	UPDATE_LINK_VALUE_ON_SRC_OBJECT	UPDATE	OBJECT
2920	UNABLE_TO_OPEN_UDP_PORT_FOR_EXCLUSIVE_USE	OPEN	PORT
2946	FETCH_GROUP_MANAGED_SERVICE_ACCOUNT_PWD	RETRIEVE	PASSWORD
2947	FAILED_TO_FETCH_GROUP_MANAGED_SERVICE_ACCOUNT_PWD	RETRIEVE	PASSWORD
2948	DROPPED_INVALID_CLAIM_FOR_GIVEN_USER	DROP	CLAIM
2951	FAILED_TO_CONFIGURE_DS	CONFIGURE	SERVICE
2952	ATTEMPT_TO_DELETE_REGISTRY_RECURSIVELY	DROP	REGISTRY

Table P-1 (Cont.) Directory Service Audit Trail Events

Event ID	Source Event	Command Class	Target Type
2953	DELETED_REGISTRY	DROP	REGISTRY
2986	APPLIED_CHANGES_IN_PACKET	UPDATE	PACKET
2987	APPLIED_OBJECT_CHANGES_IN_PACKET	UPDATE	PACKET
2988	APPLIED_LINK_CHANGES_IN_PACKET	UPDATE	PACKET
2994	DIRECTORY_SYNC_INDEX_CREATION_SUCCEEDED	CREATE	INDEX
2995	MOVED_ORPHANED_OBJECT_TO_LOSTANDFOUND_CONTAINER	MOVE	OBJECT
3001	CONFIG_ERROR_FAILING_DB_OPERATION	FAIL	DATABASE
10039	DIRLOG_BEGIN_DIR_SEARCH	SEARCH	OBJECT

P.3 Security Audit Trail Events

Security audit trail events include events such as OPERATE_OBJECT and ESTABLISH_SOURCE_NAMING_CONTEXT.

Table P-2 lists the Security audit trail events and their **command_class** and **target_type** mappings in the Oracle AVDF audit record.

Table P-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
5169	MODIFY_OBJECT	UPDATE	OBJECT