Changes in This Release for Oracle Database SQL Firewall Guide

This preface contains:

Changes in Oracle Database SQL Firewall 23ai

Oracle Database SQL Firewall Guide for Oracle Database 23ai has new security features.

Oracle SQL Firewall is Now Built into Oracle Database

Starting with Oracle Database 23ai, Oracle SQL Firewall inspects all incoming SQL statements and ensures that only explicitly authorized SQL is run.

You can use SQL Firewall to control which SQL statements are allowed to be processed by the database. You can restrict connection paths associated with database connections and SQL statements. Unauthorized SQL can be logged and blocked.

Because SQL Firewall is built into the Oracle database, it cannot be bypassed. All SQL statements are inspected, whether local or network, or encrypted or clear text. It examines top-level SQL, stored procedures and the related database objects.

SQL Firewall provides real-time protection against common database attacks by restricting database access to only authorized SQL statements or connections. It mitigates risks from SQL injection attacks, anomalous access, and credential theft or abuse.

SQL Firewall uses session context data such as IP address, operating system user name, and operating system program name to restrict how a database account can connect to the database. This helps mitigate the risk of stolen or misused application service account credentials. A typical use case for SQL Firewall is for application workloads.

You can use SQL Firewall in both the root and a pluggable database (PDB).

Updates to Oracle Database SQL Firewall 23ai

Oracle Database SQL Firewall Guide for Oracle Database 23ai as the following update.

New Procedure for Oracle SQL Firewall DBMS_SQL_FIREWALL PL/SQL Package

The Oracle SQL Firewall package `DBMS_SQL_FIREWALL` now has an additional procedure, `DBMS_SQL_FIREWALL.APPEND_ALLOW_LIST_SINGLE_SQL`.

This procedure enables you to individually append specific SQL records from a capture log or a violation log to an existing allow-list. While `DBMS_SQL_FIREWALL.APPEND_ALLOW_LIST` provides the flexibility to append the entire violation or capture log to the allow-list, in most common scenarios you might also need the flexibility to add just one of them instead of the entire list. In previous releases, if you wanted to append specific SQL commands to an allow-list, you had to use `DBMS_SQL_FIREWALL.APPEND_ALLOW_LIST` to append the entire violation or capture log to the allow-list, and then use `DBMS_SQL_FIREWALL.DELETE_ALLOWED_LIST` to manually delete the unwanted entries. This enhancement gives more flexibility to adjust the allow-list with specific records that you want to include.

Related Topics

- *Oracle Database PL/SQL Packages and Types Reference*