3

How Oracle SQL Firewall Works with Other Oracle Features

Learn how Oracle SQL Firewall works in conjunction with other Oracle features.

3.1 SQL Firewall and Audit Vault and Database Firewall (AVDF)

AVDF 20.13 and later can collect SQL Firewall violation logs.

Learn how to configure AVDF to collect SQL Firewall violation logs: Using SQL Firewall with AVDF.

3.2 Oracle SQL Firewall and Oracle Data Pump

You can use Oracle Data Pump to export and import Oracle SQL Firewall captures and allow-list metadata.

3.2.1 About Oracle Data Pump Export and Import Operations on Oracle SQL Firewall Metadata

Oracle SQL Firewall integrates with Oracle Data Pump to support the export and import of the SQL Firewall metadata, including the metadata for captures and allow-lists.

This is typically required in scenarios where the training can be done once on a non-production database, and then SQL Firewall can be enabled on multiple production databases using the allow-list that was generated during the non-production training stage.

Oracle Database maintains the status of captures and allow-lists during the export and import operations, unless you are merging an allow-list from the source database into an existing allow-list in the target database. For example, if a capture is enabled in the source database at the export time, it will be enabled in the target database after the import operation completes. This is similar if you are importing an allow-list when there is no allow-list for the same user in the target database before the import operation.

If you are merging an allow-list from the source database into an existing allow-list in the target database, the settings (such as `status`, `top_level_only`, `enforce`, and `block`) of the allow-list in the target database remain the same as before the import operation. Only the allowed SQL and contexts are merged.

For Oracle Data Pump, Oracle supports the export or import of all the existing SQL Firewall metadata (that is, captures and allow-lists) as a whole. Oracle does not support the export or import of a specific capture or a specific allow-list through Oracle Data Pump.

If you only want to export or import the allow-list for one user, from one specific database to another, then use the `DBMS_SQL_FIREWALL.EXPORT_ALLOW_LIST` or `DBMS_SQL_FIREWALL.IMPORT_ALLOW_LIST` procedure. (These two procedures do not rely on Oracle Data Pump and can be used independently.) Oracle does not support the export and import of SQL Firewall logs (that is, capture and violation logs).

3.2.2 Cases Where Oracle Data Pump Skips the Import for an Oracle SQL Firewall Capture or Allow-List

During an import operation, Oracle Data Pump will skip a particular Oracle SQL Firewall capture or allow-list and continue to import other captures or allow-lists for certain cases.

These cases are as follows:

- If the target users do not exist in the target database, then the captures and allow-lists for those non-existing users are not imported.
- If an allow-list refers to one or more current users that do not exist in the target database, then this allow-list is not imported.
- For an allow-list to be imported, if an allow-list for the same user already exists in the target database and its `top_level_only` setting is different than the allow-list to be imported, then the allow-list is not imported.
- For an allow-list to be imported, if a capture for the same user already exists in the target database and its `top_level_only` setting is different than the allow-list to be imported, then the allow-list is not imported.
- If an allow-list to be imported is enabled, and in the target database, there is an enabled capture for the same user but there is no disabled allow-list for the same user, then the allow-list is not imported to avoid having an enabled capture and an enabled allow-list for the same user at the same time.
- If a capture to be imported already exists for the same user in the target database, then the capture is not imported.
- If a capture to be imported is enabled, and there is an enabled allow-list for the same user in the target database, then the capture is not imported to avoid having an enabled capture and an enabled allow-list for the same user at the same time.
- For a capture to be imported, if an allow-list for the same user already exists in the target database and its `top_level_only` setting is different than the capture to be imported, then the capture is not imported.

3.2.3 Using Oracle Data Pump with Oracle SQL Firewall

You can use the `expdp` and `impdp` commands to export and import Oracle SQL Firewall captures and allow-lists metadata.

1. Log in to the server where SQL Firewall is used.
2. At the command line, perform the Oracle Data Pump export or import operation.
   - To export SQL Firewall metadata, use the following syntax:

     ```
     expdp user_name@pdb_name FULL=Y DIRECTORY=dumpfile_dir
     INCLUDE=SQL_FIREWALL dumpfile=dumpfile_name.dmp LOGFILE=filename.log
     ```

     In this specification:

     – `FULL=Y`, which enables full export mode. SQL Firewall metadata will be exported only with the full export mode.

  - INCLUDE=SQL_FIREWALL can be used in the INCLUDE or EXCLUDE filter. This tag is optional. It enables you to export and import just the SQL Firewall metadata from one database to another.

  For example:

  ```
  expdp "hr@hr_pdb" FULL=Y DIRECTORY=sql_fw_dumpfiles
  INCLUDE=SQL_FIREWALL DUMPFILE=sql_fw_app.dmp LOGFILE=sql_fw_app.log
  Enter password: password
  ```

- To import SQL Firewall metadata:

  ```
  impdp user_name@pdb_name FULL=Y DIRECTORY=dumpfile_dir
  INCLUDE=SQL_FIREWALL dumpfile=dumpfile_name.dmp LOGFILE=filename.log
  ```

  For example:

  ```
  impdp "hr@hr_pdb" FULL=Y DIRECTORY=dumpfile_dir INCLUDE=SQL_FIREWALL
  dumpfile=sql_fw_app.dmp LOGFILE=sql_fw_app.log
  Enter password: password
  ```

Related Topics

- *Oracle Database Utilities*

3.3 Oracle SQL Firewall and Oracle Scheduler Jobs

In most scenarios, you may want to exclude Oracle Scheduler jobs from Oracle SQL Firewall enforcement because these are not typically run by users.

By default the Oracle Scheduler jobs are excluded. You can enable or disable the enforcement of SQL Firewall during Oracle Scheduler operations by setting the FEATURE parameter to the DBMS_SQL_FIREWALL.SCHEDULER_JOB constant, using the following procedures:

- DBMS_SQL_FIREWALL.INCLUDE permits SQL Firewall to capture any SQL or enforce any allow-lists during Oracle Scheduler operations.
- DBMS_SQL_FIREWALL.EXCLUDE prevents SQL Firewall from capturing any SQL or enforcing any allow-lists during Oracle Scheduler operations.

For example:

```
EXEC DBMS_SQL_FIREWALL.EXCLUDE (DBMS_SQL_FIREWALL.SCHEDULER_JOB);
```

Related Topics

- *Oracle Database PL/SQL Packages and Types Reference*
- Oracle SQL Firewall Data Dictionary Views
  Oracle Database provides a set of data dictionary views that provide information about Oracle SQL Firewall configurations.

3.4 Oracle SQL Firewall and Oracle Database Vault

Oracle Database Vault requires special authorization before you can use Oracle SQL Firewall in a Database Vault environment.

3.4.1 Using SQL Firewall in an Oracle Database Vault Environment

Depending on the type of protection that you want to configure, you can use either or both Oracle Database Vault and SQL Firewall.

Database Vault enables you to use realms and command rules to block access to sensitive objects, the execution of critical commands, and SQL connections from untrusted factors such as the time of the day, IP address, host name, program name, or any number of identifiable attributes that are associated with the user. In a Database Vault environment, you can extend this protection by using SQL Firewall to capture an allow-list of SQL commands with an associated trusted database connection paths for a database account. Then you can log (and optionally block) the unseen SQL traffic. SQL Firewall enforcement can distinguish approved SQL statements and connections from the unauthorized SQL traffic, which adds to the protection layer that realms and command rules provide to prevent access to sensitive objects unless they have been explicitly authorized.

The following table shows a comparison of how you can enforce protections using Database Vault realms and command rules, and SQL Firewall.

Table 3-1 Comparison of Oracle Database Vault and SQL Firewall Protections

Use Case	Realms	Command Rules	SQL Firewall
Protect database schemas	Yes, traditional or mandatory realms can limit access to your data. • Entire schema or schemas • Object types • Specific objects by name	Yes, DML or DDL statements against schema objects	No
Protect database roles	Yes, traditional or mandatory realms can protect your roles.	Yes, create a command rule with `GRANT` or `REVOKE` statements for specific roles.	No
Protect database objects	Yes, traditional or mandatory realms can limit access to your data. • Entire shema or schemas • Object types • Specific objects by name	Yes, DML or DDL statements against schema objects • Entire schema or schemas • Object types • Specific objects by name	No
Protect individual SQL statements	No	Yes, control statements against schema or individual schema objects.	Yes, block all but explicitly allowed SQL statements.
Allow-list and protect application SQL traffic	No	No	Yes, block all but explicitly allowed SQL statements.
Protect against risks of compromised accounts	Yes, establish trusted path conditions based on any factors that can be checked programmatically.	Yes, protect `CONNECT` command usage.	Yes, block sessions from untrusted client IP, program and OS user name
Protect database users against SQL Injection risks	No	No	Yes, create an allow-list SQL Firewall policy for each database user and enforce it.

3.4.2 Authorization for Using SQL Firewall in an Oracle Database Vault Environment

In an Oracle Database Vault environment, users who want to configure SQL Firewall must have Oracle Database Vault-specific authorization.

When Database Vault is enabled, the management of SQL Firewall (that is, the invocation of the `DBMS_SQL_FIREWALL` package) requires SQL Firewall administrators to have Database Vault-specific authorization in addition to the `ADMINISTER SQL FIREWALL` system privilege. This requirement is to ensure that only trusted users will be able to manage SQL Firewall in a Database Vault environment.

You can authorize SQL Firewall administrators to allow or not allow captures on users who have the `DV_OWNER`, `DV_ADMIN`, or `DV_ACCTMGR` roles in a Database Vault environment. When Database Vault operations control is enabled, common users will be blocked from using SQL Firewall (that is, the `DBMS_SQL_FIREWALL` procedures for managing captures and allow-lists) on local users unless the common users are included in the exception list.

Related Topics

- *Oracle Database Vault Administrator's Guide*

3.5 Oracle SQL Firewall and Oracle Real Application Security

You can use Oracle SQL Firewall with Oracle Real Application Security (Oracle RAS) to capture SQL statements that come from an Oracle RAS application for the `XS$NULL` user.

You can generate and enforce an allow-list for the `XS$NULL` user after completing a SQL Firewall capture operation. However, SQL Firewall does not perform capture and enforce operations for Oracle RAS end-user identities.

3.6 Oracle SQL Firewall and Oracle Database Centrally Managed Users and Enterprise Users

Oracle SQL Firewall will capture a global user's activities if the SQL Firewall capture is enabled.

However, SQL Firewall does not distinguish enterprise user identities (for example, centrally managed users with Active Directory (CMU-AD) users, Oracle Cloud Infrastructure (OCI) Identity and Access Management (IAM) users, Oracle Internet Directory (OID) users, or Microsoft Azure Active Directory users).

3.7 Oracle SQL Firewall and Oracle Virtual Private Database

When Oracle Virtual Private Database policies are run, Oracle SQL Firewall captures SQL commands right after their executions.

However, SQL Firewall does not consider any modification or transformation that is made by the database kernel (for example, views, synonyms, SQL macro expansion, Virtual Private Database enforcement, and so on). You should train SQL Firewall to capture all the expected incoming SQL statements to formulate the allow-list.

3.8 Oracle SQL Firewall in a Multitenant Environment

Oracle SQL Firewall is affected at both the CDB root level and the individual PDB level.

You can run the SQL Firewall processes and set SQL Firewall trace events in both the CDB and individual PDBs.

In the CDB root:

- You can enable SQL Firewall in the CDB root container, and then create SQL Firewall policies, enable or disable SQL Firewall, start or stop captures, and enable or disable allow-lists. These settings apply to the CDB root only.
- In an Oracle Database Vault operations control environment, there are no restrictions in using SQL Firewall.

In individual PDBs:

- You can enable SQL Firewall in an individual PDB, and then create SQL Firewall policies, enable or disable SQL Firewall, start or stop captures, and enable or disable allow-lists. These settings apply to the current PDB only.
- In a Database Vault operations control environment, common users cannot start or stop captures on local users, nor can they enable or disable allow-lists on local users.