

Contents

Preface

Documentation Accessibility	vii
Diversity and Inclusion	vii
Related Documents	vii

Changes in This Release for Oracle Database SQL Firewall Guide

Changes in Oracle Database SQL Firewall 23ai	ix
Updates to Oracle Database SQL Firewall 23ai	ix

1 Overview of Oracle SQL Firewall

1.1 About Oracle SQL Firewall	1-1
1.2 Licensing Oracle SQL Firewall	1-3
1.3 Getting Started with Oracle SQL Firewall	1-3
1.4 Privileges for Configuring and Using Oracle SQL Firewall	1-5
1.5 Getting Hands-On Experience with Oracle SQL Firewall	1-5

2 Configuring Oracle SQL Firewall

2.1 Configuring and Managing Oracle SQL Firewall with the DBMS_SQL_FIREWALL Package	2-1
2.1.1 Configuring Oracle SQL Firewall Using the DBMS_SQL_FIREWALL Package	2-1
2.1.2 Modifications to Oracle SQL Firewall Configurations	2-5
2.1.3 Managing Performance for Capture Logs	2-7
2.1.4 Purging Oracle SQL Firewall Logs	2-7
2.1.5 Auditing Oracle SQL Firewall Violations by Using Unified Audit Policies	2-8
2.1.6 Troubleshooting Oracle SQL Firewall by Enabling or Disabling SQL Firewall Trace Files	2-9
2.2 Configuring and Managing Oracle SQL Firewall with Oracle Data Safe	2-9
2.2.1 SQL Firewall Overview	2-10
2.2.1.1 About SQL Firewall	2-10
2.2.1.2 Terms in SQL Firewall	2-11
2.2.1.3 Prerequisites for SQL Firewall	2-12

2.2.2	Start Using SQL Firewall	2-12
2.2.2.1	Step 1: Enable SQL Firewall On Your Target Database	2-13
2.2.2.2	Step 2: Start SQL Collection for a Database User	2-13
2.2.2.3	Step 3: Monitor the Progress of SQL Collection with Insights	2-13
2.2.2.4	Step 4: Generate and Enforce SQL Firewall Policies	2-15
2.2.2.5	Step 5: View SQL Firewall Violation Reports	2-16
2.2.2.6	Step 6 (Optional): Create Audit and Alert Policies for SQL Firewall Violations	2-18
2.2.2.7	Step 7 (Optional): Configure Notifications for SQL Firewall Violations	2-18
2.2.3	Gain Insights from SQL Firewall	2-20
2.2.3.1	View the SQL Firewall Dashboard	2-20
2.2.3.2	View Violations	2-21
2.2.3.3	Follow-Up Actions for SQL Firewall	2-23
2.2.4	Manage SQL Firewall	2-23
2.2.4.1	Update the Database Security Configuration	2-23
2.2.4.2	Purge a SQL Collection	2-24
2.2.4.3	Drop a SQL Collection	2-24
2.2.4.4	View and Manage SQL Firewall Policies	2-25
2.2.4.5	Update SQL Firewall Policies	2-26
2.2.4.6	Update the Enforcement of SQL Firewall Policies	2-27
2.2.4.7	Disable or Enable SQL Firewall Policies	2-28
2.2.4.8	Drop SQL Firewall Policies	2-28
2.2.5	View and Manage Violations Report	2-28
2.2.5.1	Modifying Columns in a Violations Report	2-28
2.2.5.2	Basic Filtering in a Violations Report	2-29
2.2.5.3	Advanced Filtering in a Violations Report	2-29
2.2.5.4	Tips for Using the Filter Builder to Create Advanced Filters	2-30
2.2.5.5	Create a Custom Violations Report	2-31
2.2.5.6	Update a Custom Violations Report	2-31
2.2.5.7	Delete a Custom Violations Report	2-31
2.2.5.8	Create or Manage a Schedule for a Violations Report	2-32
2.2.5.9	View and Manage Violation Report History	2-32
2.2.6	Create and Modify Event Notifications in SQL Firewall	2-33
2.2.6.1	Creating Event Notifications for SQL Firewall	2-33
2.2.6.2	Modifying Event Notifications For SQL Firewall	2-34

3 How Oracle SQL Firewall Works with Other Oracle Features

3.1	SQL Firewall and Audit Vault and Database Firewall (AVDF)	3-1
3.2	Oracle SQL Firewall and Oracle Data Pump	3-1
3.2.1	About Oracle Data Pump Export and Import Operations on Oracle SQL Firewall Metadata	3-1

3.2.2	Cases Where Oracle Data Pump Skips the Import for an Oracle SQL Firewall Capture or Allow-List	3-2
3.2.3	Using Oracle Data Pump with Oracle SQL Firewall	3-2
3.3	Oracle SQL Firewall and Oracle Scheduler Jobs	3-3
3.4	Oracle SQL Firewall and Oracle Database Vault	3-3
3.4.1	Using SQL Firewall in an Oracle Database Vault Environment	3-4
3.4.2	Authorization for Using SQL Firewall in an Oracle Database Vault Environment	3-5
3.5	Oracle SQL Firewall and Oracle Real Application Security	3-5
3.6	Oracle SQL Firewall and Oracle Database Centrally Managed Users and Enterprise Users	3-5
3.7	Oracle SQL Firewall and Oracle Virtual Private Database	3-5
3.8	Oracle SQL Firewall in a Multitenant Environment	3-6

4 Oracle SQL Firewall Data Dictionary Views and Example Queries

4.1	Oracle SQL Firewall Data Dictionary Views	4-1
4.2	Query to Find a User's Allowed SQL and Accessed Objects	4-2
4.3	Query to Find a User's Allowed IP Address	4-2
4.4	Query to Find a User's Oracle SQL Firewall Violations	4-2

Part I Appendix: SQL Firewall Database Views and DBMS Package

A SQL Firewall Database Views

A.1	DBA_SQL_FIREWALL_ALLOW_LISTS	A-1
A.2	DBA_SQL_FIREWALL_ALLOWED_IP_ADDR	A-1
A.3	DBA_SQL_FIREWALL_ALLOWED_OS_PROG	A-2
A.4	DBA_SQL_FIREWALL_ALLOWED_OS_USER	A-2
A.5	DBA_SQL_FIREWALL_ALLOWED_SQL	A-2
A.6	DBA_SQL_FIREWALL_CAPTURE_LOGS	A-3
A.7	DBA_SQL_FIREWALL_CAPTURES	A-4
A.8	DBA_SQL_FIREWALL_SESSION_LOGS	A-5
A.9	DBA_SQL_FIREWALL_SQL_LOGS	A-5
A.10	DBA_SQL_FIREWALL_STATUS	A-5
A.11	DBA_SQL_FIREWALL_VIOLATIONS	A-6

B DBMS_SQL_FIREWALL

B.1	DBMS_SQL_FIREWALL Overview	B-1
B.2	DBMS_SQL_FIREWALL Security Model	B-1
B.3	DBMS_SQL_FIREWALL Constants	B-2
B.4	Summary of DBMS_SQL_FIREWALL Subprograms	B-3

B.4.1	ADD_ALLOWED_CONTEXT Procedure	B-4
B.4.2	APPEND_ALLOW_LIST Procedure	B-5
B.4.3	APPEND_ALLOW_LIST_SINGLE_SQL Procedure	B-6
B.4.4	CREATE_CAPTURE Procedure	B-8
B.4.5	DELETE_ALLOWED_CONTEXT Procedure	B-9
B.4.6	DELETE_ALLOWED_SQL Procedure	B-10
B.4.7	DISABLE Procedure	B-10
B.4.8	DISABLE_ALLOW_LIST Procedure	B-11
B.4.9	DROP_ALLOW_LIST Procedure	B-11
B.4.10	DROP_CAPTURE Procedure	B-12
B.4.11	ENABLE Procedure	B-12
B.4.12	ENABLE_ALLOW_LIST Procedure	B-13
B.4.13	EXCLUDE Procedure	B-14
B.4.14	EXPORT_ALLOW_LIST Procedure	B-14
B.4.15	FLUSH_LOGS Procedure	B-15
B.4.16	GENERATE_ALLOW_LIST Procedure	B-16
B.4.17	IMPORT_ALLOW_LIST Procedure	B-17
B.4.18	INCLUDE Procedure	B-18
B.4.19	PURGE_LOG Procedure	B-18
B.4.20	START_CAPTURE Procedure	B-19
B.4.21	STOP_CAPTURE Procedure	B-20
B.4.22	UPDATE_ALLOW_LIST_ENFORCEMENT Procedure	B-20

Index
