Oracle® Audit Vault and Database Firewall

Concepts Guide

Release 20
E93407-12
February 2024

ORACLE

Oracle Audit Vault and Database Firewall Concepts Guide, Release 20

E93407-12

Contents

Preface

Oracle Audit Vault and Database Firewall Concepts Guide introduces the concepts and terminology used in Oracle Audit Vault and Database Firewall (also referred to as Oracle AVDF). This document provides an overview of the main features used by Database Auditors, Database Administrators, and developers.

Audience

This document is an overview of the product capabilities and is intended for security managers, audit managers, and database administrators (DBAs) who are involved in the selection of database activity monitoring solutions and deployment of Oracle Audit Vault and Database Firewall.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

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.

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

1

Overview of Oracle Audit Vault and Database Firewall

Monitoring database activity to support incident investigation, detect potentially malicious behavior, and fulfill regulatory requirements is essential. Enabling either database auditing or monitoring network events can help you to get this visibility.

Database Activity Monitoring (DAM) is a security technology for monitoring and analyzing database activity. DAM solutions are used to identify and report on fraudulent, illegal, or other undesirable behavior and typically used to address security and compliance needs.

Oracle Audit Vault and Database Firewall (Oracle AVDF) supports native database audit data collection and network-based SQL monitoring to deliver a comprehensive Database Activity Monitoring solution.

Activity monitoring is essential, but organizations are also worried about the security posture of their databases. Were best practices followed when configuring the databases? Are databases in compliance with security standards? What else should be considered to strengthen the Oracle Database further? Database security posture management (DSPM) helps answer those questions, combining the ability to assess database configuration and security settings with sensitive data discovery to provide an integrated picture of a database's risk and security posture.

Oracle AVDF 20.9 and later expands the product's capabilities from database activity monitoring (DAM) to database security posture management (DSPM).

Oracle AVDF expands beyond database activity monitoring to manage your Oracle Database's security posture. AVDF's best-in-class activity monitoring capabilities are enhanced with visibility into security configuration, user entitlements, stored procedures, and how much and what types of data are in the database.

Use Cases

There are two key use cases for Database Activity Monitoring, namely, compliance and corporate security guidelines.

- Corporate security guidelines: While corporate security guidelines vary, they often require setting baseline database security configuration and detecting deviation, discovering sensitive objects and privileged users, auditing privileged user activity, logon, and logoff events, sensitive data access, monitoring database traffic, preventing SQL injection attempts, and many other common security-relevant activities. These guidelines typically require both database auditing and network-based SQL traffic monitoring capabilities
- Accelerate regulatory compliance: Organizations need to address the requirements of regulations such as GDPR, PCI, GLBA, HIPAA, IRS 1075, SOX, and UK DPA. These regulations require complete visibility of activities on sensitive objects, privileged users, value change auditing, data structure changes, etc. Database auditing and network-based SQL traffic must be monitored as part of the regulatory requirements to give this level of visibility for the forensic analysis of security events.

1.1 Database Auditing and Network Based SQL Traffic Monitoring: Why Both Are Needed

Database Auditing

Database auditing involves creating and enabling database policies to track the actions taken on database objects or users. When auditing is enabled, database activities on specified objects and users produce an audit trail of these operations. Each action generates an audit record that includes what database operation was performed, who performed the operation, the database objects involved, time of execution, and the SQL statement itself. Database auditing not only captures local activity but also any database activity that does not cross the network as SQL, such as logging local or remote console connection, to make database and user changes.

Network Based SQL Traffic Monitoring

SQL injection is perhaps the most common method used to attack databases by exploiting application vulnerabilities. SQL injection exploits flaws in application code—the application that sends SQL statements to a database. Given that much of that application code is written without analyzing possible SQL injection issues, many applications are exposed to vulnerabilities.

Database Firewall can be used to monitor and analyze the SQL traffic to the database, whether coming from an application server or a user connecting to the database directly. By monitoring and analyzing the SQL statements, the database firewall can intercept SQL statements generated as a result of a SQL injection attack, block or substitute them with other SQL statements, thereby thwarting SQL injection attack. As SQL statements are evaluated for policy compliance and the actions are taken over the network it does not consume resources on the database server.

In many instances, corporate or regulatory policies may require that trusted path access to corporate applications should be enforced. This could involve only allowing application access to the database from certain IP addresses or users. Database Firewall policies can be used to monitor, alert, block, and substitute SQL statements based on user session information, such as IP address or database user name. You can also use the Database Firewall to train it to understand normal or approved SQL, and block anything else that is different.

Why Both

Oracle recommends a holistic approach to Database Activity Monitoring, requiring both database auditing and SQL traffic monitoring. Auditing typically captures detailed information after a certain event has occurred, while monitoring SQL traffic helps you monitor the SQL statement before it reaches the database, making it possible to block suspicious statements. Both of them give different views into the same event, one after, and one before. You can start with either capability and expand their architecture to include both.

1.2 Oracle Audit Vault and Database Firewall Components

Oracle Audit Vault and Database Firewall (Oracle AVDF) has three main components: Audit Vault Server, Audit Vault Agents, and Database Firewall.

Audit Vault Server

The Audit Vault Server is a mandatory component of AVDF. Every AVDF installation has at least one Audit Vault Server. This server has the following components:

- A hardened Oracle Linux operating system
- An Oracle Database, which serves as the audit repository. The audit repository database is encrypted using Oracle Transparent Data Encryption and protected with Oracle DatabaseVault.
- The AVDF application, which provides the interface for the AVDF console and the Audit Vault Command Line Interface (AVCLI).

The Audit Vault Server is the central repository of audit records and events captured by the Database Firewall. The Audit Vault Server performs four primary functions:

- For Oracle databases, it captures both before and after values, as well as changes to user entitlements and stored procedures. Similarly, for Microsoft SQL Server (Oracle AVDF 20.9 and later) and MySQL (Oracle AVDF 20.11 and later), it captures before and after values, along with stored procedures. The support for pre-seeded audit policies further facilitates the implementation of auditing best practices.
- Default predefined reports with customization capabilities: Audit Vault Server provides dozens of default reports including changes to database configuration, security, and user entitlements. It also provides reports on login and logout, sensitive data access and modification, stored procedure changes, and many more. Report data can be easily filtered and searched for investigations. Using predefined compliance reports for GDPR, PCI, GLBA, HIPAA, IRS 1075, SOX, and UK DPA, you can easily provide needed reports to auditors. Third-party reporting tools can connect to the Audit Vault Server schema for further analysis.
- Configuring alerts and notifying when certain events occur: Audit Vault Server raises alerts on user-specified events such as multiple failed login attempts, sensitive table access by unauthorized users, and data export operations. Custom alerts can be configured in Oracle AVDF.
- Oracle AVDF supports information life cycle management (ILM) policies to help organizations meet compliance requirements. Per target policies can be created specifying the online and offline retention periods, and based on that, activity data is automatically moved from the Audit Vault Server to the archive. If necessary, data in the archive location can be restored to the Audit Vault Server, and this data then becomes visible in the reports.

Audit Vault Server supports a high-availability architecture to ensure that audit record collection does not stop. A secondary audit vault server can be configured so that in the event of a failure of the primary, the secondary becomes the primary without any manual intervention.

Audit Vault Agent

Audit Vault Agent retrieves audit data from audit trails (sources of audit data) for various types of targets and sends the audit data to the Audit Vault Server. For directory-based trails, the Audit Vault Agent is deployed on the same machine as the trail, and for database table based trails it can be deployed on a remote machine. A single Audit Vault Agent can collect from multiple targets and trails.

Audit trails include database audit trails, OS trails, and directory trails. Database audit trails include Oracle Database, Oracle Autonomous Database, Microsoft SQL Server, SAP

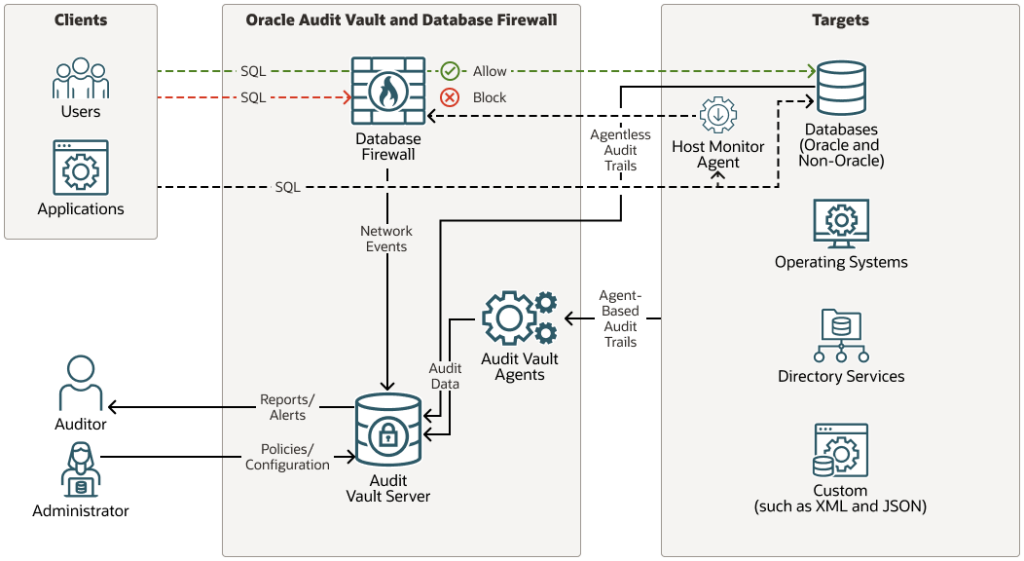
Sybase, IBM Db2 for LUW, MySQL, MongoDB and PostgreSQL. The audit data can come from audit tables or files. Oracle AVDF can also capture before and after values from REDO records of Oracle databases, Microsoft SQL Server (Oracle AVDF 20.9 and later), and MySQL (Oracle AVDF 20.11 and later). OS audit trails include Oracle Linux, Red Hat Linux, Oracle Solaris, Microsoft Windows, and IBM AIX. You may use the QuickCSV collector (AVDF 20.11 and later) to collect audit data from MariaDB, EnterpriseDB (Postgres), and other systems that create audit data in CSV.

> **Note:**
>
> Starting in Oracle AVDF 20.9, you can use agentless collection instead of the Audit Vault Agent for up to 20 Oracle Database table audit trails. Starting in Oracle AVDF 20.10, you can also use agentless collection for Microsoft SQL Server directory audit trails for `.sqlaudit` and `.xel` (extended events). The total number of audit trails for agentless collection should not exceed 20. See Adding Audit Trails with Agentless Collection.

Database Firewall

Database Firewall inspects SQL traffic going into the database and determines with high precision whether to allow, log, alert, substitute, or block the SQL. Database Firewall events are stored in the Audit Vault Server and consolidated with the audit data giving you a unified view into all activities. The Database Firewall is covered in detail in the next chapter.

Figure 1-1 Oracle AVDF Architecture



1.3 Database Security Posture Management

Database security assessments are essential because they help identify security risks that can compromise the confidentiality, integrity, and availability of data. However, conducting thorough and periodic evaluations is frequently challenging, especially

when you're not just managing 10–20 databases but are responsible for hundreds or thousands of them. Complex database systems can make it difficult to identify potential vulnerabilities and threats consistently. Another challenge is the availability of skilled personnel to perform and evaluate comprehensive security assessments.

AVDF - Database security posture management (DSPM) provides a fleet-wide simplified and centralized view of security configuration assessments for Oracle Database, along with security findings and associated risks. Summarized risk findings help prioritize and guide immediate action on potential risks associated with the Oracle Database fleet. AVDF also assists you in discovering sensitive data and privileged users in the Oracle Database.

1.4 Enterprise Deployment

Delivered as a pre-configured software appliance, Oracle AVDF can be installed on an x86 hardware of choice giving you the scale you need. Periodic release updates for Oracle AVDF include updates to the embedded operating system, Oracle database, and the Oracle AVDF application itself simplifying its maintenance. Further, Audit Vault Server automatically updates the agents used for collecting audit data and eliminates administrator involvement. You can use the rich command-line interface to automate administrative operations.

Audit Vault Server can consolidate audit data and firewall events from hundreds or thousands of databases and operating systems. It can be deployed in active-standby mode, ensuring availability. You can configure the data archival policies to automatically archive historic data to low-cost storage and retrieve it as needed.

Beyond hardened configuration, Oracle AVDF encrypts the collected data using Transparent Data Encryption, encrypts the network traffic, uses Database Vault to restrict access to data, and provides separation of duties between the administrator and the auditor.

1.5 Hybrid Cloud Support

Organizations increasingly face the situation where some of their databases are deployed on-premises while others are deployed in the cloud. The challenge is to audit and monitor them all, ideally with a single console. Utilizing a solution deployed on-premises for both on-premises and cloud database targets has many advantages including consistent policies, unified reporting, and common alert management. Existing alert configurations and data retention polices can be applied for cloud databases. For you the main benefit here is that the cloud vendor cannot modify the audit data, and thus you have an independent view of the events on your cloud databases. Thus, you get full control, and have complete view over your audit data using one single unified dashboard.

1.6 Provisioning Audit Policies for Oracle Databases

Databases contain sensitive data – data whose access should be controlled and monitored. Examples of sensitive data might include financial reports, credit card numbers, email addresses, and data that describes an employee or customer. Sensitive data access auditing presents a powerful monitoring mechanism providing visibility into access and changes of sensitive data within the organization, and serves as a primary deterrence to those who do not have a business reason to access or modify them.

Users, some of whom may be privileged, access databases – for example, database administrators (DBAs) are frequently considered privileged users because of their broad access within the database. Privileged user accounts are often a soft target for hackers attempting to gain access to critical systems and data. Continuous privileged user activity

auditing allows security teams to easily identify any anomalous behavior and quickly detect leaks of sensitive data.

Databases users are granted privileges to perform operations within the database, and some of those privileges may be considered powerful like system privileges whose usage should be constantly monitored. Few other noteworthy actions in the database includes multiple failed login attempts, schema changes, and so on. Such actions within the database that warrant greater scrutiny and constant monitoring because it can potentially be abused are categorized into security-relevant events. A surveillance mechanism of such susceptible actions in the database constitutes security-relevant events auditing, and helps detect anomalous activities in the database very efficiently.

Focusing audit configuration on sensitive data access, privileged user activity and security-relevant events helps build better audit policies - polices that are focused on the activity that matters, selective enough to reduce the creation of unnecessary audit records, and effective enough to let you meet your audit goals.

While Oracle AVDF provides support for both unified audit and traditional, we will focus on unified auditing, as Oracle recommends that you use unified auditing going forward. For provisioning unified audit policies, Oracle AVDF provides the following three categories:

- Core Audit policies: These are policies recommended by Oracle AVDF pertaining to capturing critical database activity such as creating users, creating roles, and altering profile, database schema changes, logon events for specified users, all admin activity, and user activity for a list of specified users. With a single click, you could enable auditing for privileged users from Oracle AVDF. Oracle AVDF creates the selected policy in the target and enables it.
- Oracle predefined policies: Oracle Database provides several pre-created unified audit policies that cover common security relevant audit settings, such as logon failures, database parameter changes, modifications to user accounts and privileges, and other activities. These pre-created policies can be enabled from Oracle AVDF in addition to the core policies.
- Custom Policies: You can also develop custom unified policies in the target database that are specific to your schema and auditing needs. For example, some users may create custom audit policies that monitor select activity on specific sensitive tables by privileged users. These custom developed policies can be enabled or disabled on target databases from Oracle AVDF.

1.7 Monitoring Oracle Database Entitlements

Tracking changes in entitlements is important for many reasons, such as identifying potentially malicious activities and taking corrective action before they occur, or mistakes made by the DBA in granting certain roles to users which should not have been done. In other cases, tracking entitlement changes is useful for forensics to understand why certain users got access to tables they should not have been given.

For Oracle Databases, Oracle AVDF provides the ability to retrieve entitlement settings on a scheduled basis and compare them to understand changes. The entitlement data contains information pertaining to the creation and changes to users, roles, privileges, profiles, and other objects. Using the entitlement report, you can look at all the entitlement changes of a user during a specific time period, for example to understand how they were able to view data they were not authorized to do so.

1.8 Monitoring Oracle Stored Procedures

Stored procedure contain some of the important business or data access and modification logic. It is therefore very important to understand if any of these procedures have been modified or deleted.

Using Oracle AVDF, you can periodically check the Target to understand stored procedure creation, deletion and modifications. Oracle AVDF provides the ability to track stored procedure changes and details pertaining to when it happened and by whom.

1.9 Summary

Oracle Audit Vault and Database Firewall helps organizations increase security by proactively assessing the security posture of databases, monitoring database activity on the network and inside the database, protecting against SQL injection threats, consolidating audit data into a secure and scalable repository, and automating reporting to support audit and compliance activities.

AVDF was already a best-in-class provider for database auditing and activity monitoring platform. Now with comprehensive security-posture management for your enterprise, the discovery of sensitive data, and privileged user capabilities, AVDF becomes a one-stop solution for assessing, discovering, monitoring, and protecting the most critical asset of an organization—its data. Oracle AVDF includes an enterprise quality audit data warehouse, host-based audit data collection agents, powerful reporting and analysis tools, alert framework, audit dashboard, and a multistage Database Firewall. Users can leverage the pre-seeded policies to quickly enable database auditing with a single click.

The next chapter will discuss the Database Firewall and how you can use it to monitor and block SQL traffic before it is executed in the database.

1.10 Support Policy When Additional or Third Party Software is Installed on Oracle AVDF

Oracle Audit Vault and Database Firewall (Oracle AVDF) is shipped as an appliance, and no third-party software should be installed on the Audit Vault Server. Oracle does not test or certify any additional or third party software on Oracle AVDF. If third party software is installed, and results in problems with the Audit Vault Server and/or Database Firewall, then Oracle may not be able to help you recover the system. In cases where we believe the third party software has contributed to an issue, we may ask you to reproduce the issue on an Oracle AVDF system that does not include the third-party software.

During patching or upgrade of Oracle AVDF, you may find that the presence of third party software contributes to difficulties in completing the operation. You may also find that the process of patching/upgrading Oracle AVDF causes third party software to malfunction or cease to work altogether. Oracle AVDF upgrades also update the underlying operating system and may remove any custom libraries added by third party software.

Audit data is particularly sensitive, and loss of an audit data may result in inability to support compliance reporting and forensic investigations. In the event that you choose to install third party software on Oracle AVDF, then Oracle recommends you take additional appropriate precautions such as more frequent backups that may reduce the damage in the event the third-party software causes system instability or corruption.

2

Network-Based SQL Traffic Monitoring with Database Firewall

It's impractical to audit every operation in a database, so a solution focused only on auditing can't see the bigger picture of all database activity needed to identify anomalies, help identify suspicious activity, and block if any unauthorized activity is happening on your enterprise database.

Database Firewall is a multistage firewall that inspects SQL traffic going into the database and determines with high precision whether to allow, log, alert, substitute, or block the SQL. The SQL traffic goes through multiple stages including checks for the IP address, database or OS user, program name, SQL statement category, such as data definition language (DDL) and data manipulation language (DML), and database tables being accessed. It blocks and alerts both deny-listed SQL and SQL that is not in the allowed set of allowlist SQL statements, helping prevent SQL injection attacks.

Successful deployment of the Database Firewall depends on deciding an effective firewall policy and selecting the appropriate firewall deployment as described below.

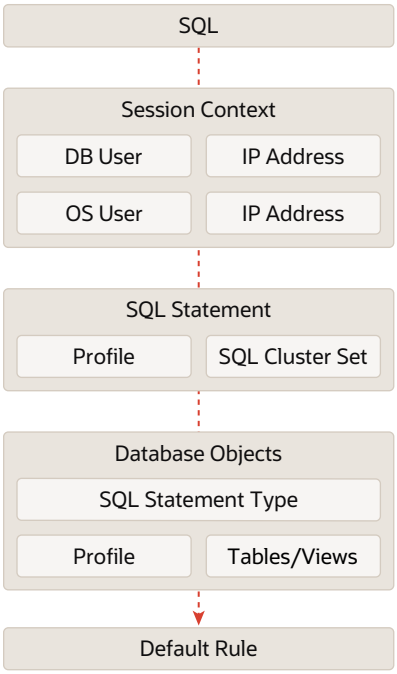
2.1 Developing an Effective Firewall Policy

Prior to deciding the policies, you need to consider who are the actors, what actions they can perform, and what actions you want the firewall to take when that action happens. Based on this, you can create the firewall policy to implement this behavior.

How Policies Are Executed in the Database Firewall: Database Firewall evaluates the SQL statement, and at each stage of the firewall, if there is a match, then the actions as specified at that stage are executed, otherwise, the SQL statement is passed on to the next stage for evaluation.

The firewall policy consists of one or more rules such as Session Context rule, SQL Statement rule, Database Object rule and Default policy rule, and are evaluated in the following order:

Figure 2-1 Order of Execution of Rules



1. **Session Context Rule**
   Session Context provides a means of allowing or denying a SQL statement based on sets of sessions attributes, without looking at the specific SQL statement. Session Context rules override all other policy rules. This rule does not look at the structure of the SQL statement, but uses database session attributes such as IP address, database users, OS users and database clients as actors to make a decision.

   Session Context rules can be used to allow specific traffic from trusted application paths without requiring them to go through further processing in the Database Firewall policy engine. Typical use-case includes:

   - Allow SQL requests from a trusted set of allow-listed client IPs to be executed by the database.
   - Allow SQL requests from trusted set of application users to be executed by the database Combining multiple sets, such IP with database user or IP with OS user, provides flexibility in narrowing down the permitted traffic through the Database Firewall. Actions can be taken on any SQL traffic, which matches the condition defined by a combination of these session attributes, such as, blocking, alerting, or logging. In the case of alerts, the threat severity level can be specified. This is explained in detail in the section below titled Actions Taken When SQL Statement Matches the Policy. SQL statements that do not match the specified conditions are forward to the next stage of the firewall for execution, namely, the SQL statement rule.

2. **SQL Statement Rule**
   The next stage of the Database Firewall uses a SQL grammar based engine to parse the SQL statement and take actions as specified in the policy. It groups SQL statements with the same grammatical structure into clusters. For example, a SQL query that searches for a specific order number 234324 is essentially the same as the one that searches for another order number 333221. Understanding the

similarity between different statements, the Database Firewall can take a policy and apply it to hundreds of equivalent SQL statements.

The Database Firewall can be trained to take a set of SQL statements and group them into similar clusters. Groups of clusters are referred to as SQL cluster sets and are useful in creating policies. SQL cluster sets provides the flexibility to group the clusters so that you can enforce policy rules on them.

SQL statement rule combines SQL cluster set, and profile, which is defined as a combination of database session attributes such as IP address, database users, OS users, and database clients.

SQL Statement rules can be used to allow SQL traffic from trusted application paths to be executed by the database. Allow-lists of normal behavior could be created by running the Database Firewall in training mode where it logs unique SQL statements and captures a set of expected SQLs representing normal traffic, such as the set of SQLs generated in a test or QA system. These groups of SQLs, called SQL Clusters, can be used in creating the policies. Typical use-case include:

- Allow allow-listed application SQL requests from a trusted set of application users.
- Allow specific allow-listed SQL requests from trusted set of privileged users accessing using a tool such as Oracle SQL Developer.

Actions that can be taken when a SQL statement matches the SQL statement rule are the same as that mentioned above for the Session context rule. It is explained in the section below titled Actions Taken When SQL Statement Matches the Policy. SQL traffic that does not match is sent to the next stage for processing, namely, the Database Object based rule.

3. **Database Object Based Rules**
Database Object based rules are used to prevent or allow specific types of SQL statements such as DML and DCL, on specific database objects such as tables and views. These rules are often used for controlling behavior of privileged users over the network where it might be necessary to stop them from accessing specific sensitive application database objects.

   Typical use cases include:

   - Allow only `SELECT` on application tables but alert or block if there are attempts to perform data modification on sensitive application tables.
   - Alert on any data modification attempts over the network that has not been allow-listed in the SQL statement rule. Actions that can be taken when a SQL statement matches the Database Object Based rule are the same as that mentioned above for the Session context rule. It is explained in the section below titled Actions Taken When SQL Statement Matches the Policy. SQL traffic that does not match is sent to the next stage for processing, namely, the Default rule.
   - Identify potential data exfiltration attempts by monitoring and alerting on the number of rows returned by the database in response to SQL `SELECT` queries (starting from Oracle AVDF 20.3).

   Monitoring the behavior of privileged users over the network and preventing them from accessing sensitive application database objects they are not authorized to access. For example, allowing only `SELECT` query on application tables, and block the SQL modifying sensitive application tables. This can be achieved using the Database Object rule. This is used to block or allow specific types of SQL statements (DML, DDL, etc.) on specific database objects such as tables and views.

In addition to monitoring access to specific sensitive tables by privileged users, Database Firewall can be used to identify exfiltration attempts by capturing the number of rows returned (starting Oracle AVDF 20.3) and used for configuring alerts. For example, if the number of returned rows exceed a threshold on a specific sensitive table, an alert can be generated. Additionally, the returned row count can be used in reports for forensic analysis.

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

4. **Default Rule**
   The Default rule is executed if the SQL statement does not match any of the other rules defined, that is, session context, SQL statement, or database object. In this case, the actions specified, logging level, and threat severity are applied to this SQL statement similar to what is mentioned for the other policies and explained in detail below.

Actions Taken When SQL Statement Matches the Policy

Each of the above Firewall policy rule defines an action to be taken by the Database Firewall in case the conditions defined by the policy match. Action taken on SQL statements can be summarized as follows:

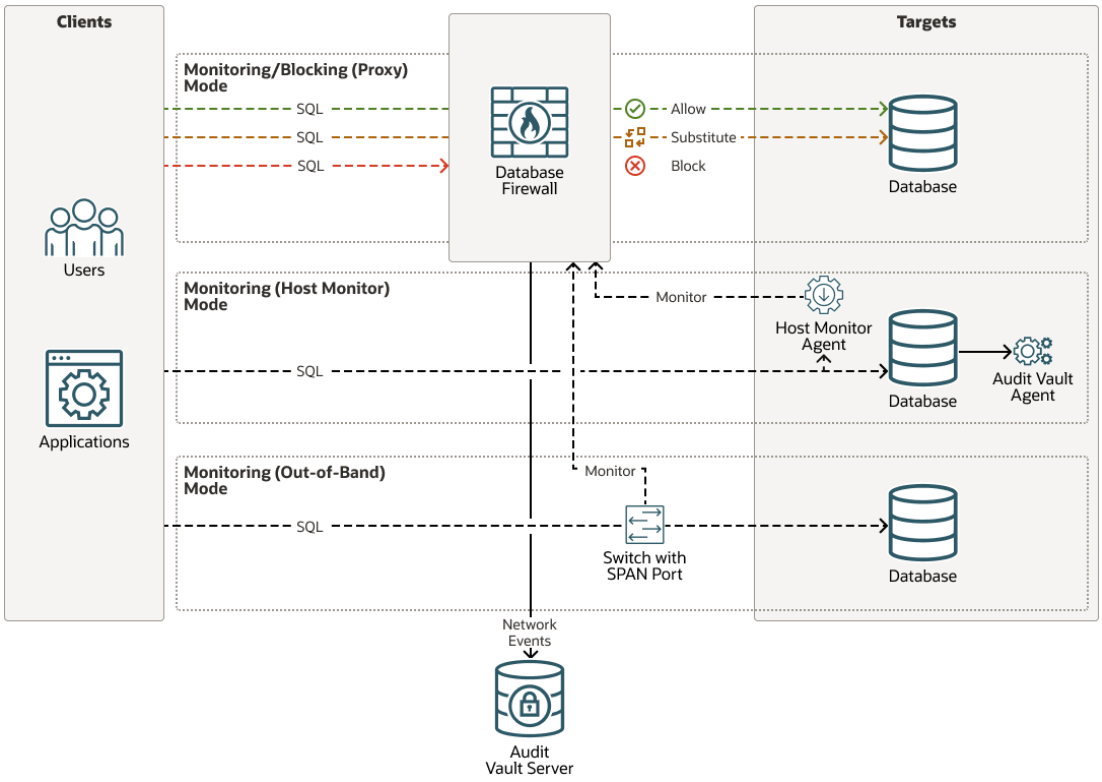
1. Action:
   - Pass: In this case, the SQL statement is passed on to the target for processing.
   - Alert: The SQL statement is sent to the Audit Vault Server as an alert, with the specified threat severity.
   - Block: The SQL statement is blocked, and the user can specify a substitute statement to execute against the target.
2. Logging level: This information is sent to the Audit Vault Server. Specifies whether or not to log the event and forward it to the Audit Vault Server.
3. Threat Severity: Threat level assigned to the Warning Database Firewall policy is essentially a multistage filtering mechanism formed by a combination of rules such as Session Context, SQL Statement, Database Object and Default rules. In each rule, you define conditions, and action to take when the SQL traffic matches that condition.

2.2 Choosing the Firewall Deployment

As part of defining the policy, you also need to decide if you want to only monitor and record the SQL statement or block it as well. Depending on that choice, you have three deployment modes, Monitoring/Blocking(Proxy), Monitoring (Host Monitor), or Monitoring (Out-of-Band).

See the below image and the following description to learn more about the different deployment modes.

Figure 2-2 Oracle AVDF Database Firewall Deployment Methods



1. **Monitoring and Blocking in Proxy Mode**
   In this mode, the Database Firewall can both monitor and block SQL, as well as optionally substitute SQL statements. Database Firewall is configured as a proxy, so that all the traffic to the database server is routed through the Database Firewall. Database clients connect to the database firewall proxy that in turn connects to the database server, forwarding all data received from the database client. In all cases, the database server identifies the database firewall as the client.

   The clients must be reconfigured to connect to the database firewall instead of the database so that the firewall can intercept all traffic and based on the policies defined, take the necessary actions. Oracle recommends that you configure the database to reject all connections that do not come from the Database Firewall to ensure that all traffic can be routed via the firewall and policies can be applied to the SQL before it is executed in the database.

   To simplify the modification required for applications to connect to the database firewall proxy mode deployments, configure local domain name servers (DNS) to resolve fully qualified domain name of the target database to the IP address of the database firewall.

   If you want to only monitor the SQL traffic, you have two other choices of deployment: Out-of-band or Host Monitor.

2. **Monitoring with Host Monitor**
   Host Monitor captures SQL traffic going to the database by monitoring and capturing traffic received by the network interface card on the database. This helps to capture relevant traffic as compared to capturing all the network traffic from an out-of-band, that is, span port, technology. The Host Monitor gets a copy of SQL traffic and hence it can only monitor and cannot block them. This SQL event data is securely sent over the

network to a database firewall. The data is then available for reports generated by Oracle AVDF.

Host monitoring is designed for situations where network reconfiguration required for out-of-band deployment mode is ruled out due to complexity.

3. **Monitoring in Out-of-Band Mode**
When you configure database activity monitoring in out-of-band mode, the database firewall listens to the network traffic, including client requests to the database and the response from the database. The database activity is monitored as per the defined policy. There are several technologies that can be used to send a copy of the database traffic to the database firewall. These technologies include, but are not limited to, span ports, network taps, and using packet replicators.

   In this mode, Oracle Database Firewall can monitor and alert on SQL traffic, but cannot block or substitute SQL statements. The out-of-band monitoring mode is the simplest deployment mode for a non-blocking policy requirement. There is no additional load on the database or the clients. There is no latency or single point of failure introduced by the Database Firewall.

2.3 Summary

Deploying the Database Firewall requires two steps:

- Deciding whether you want to only monitor and record the SQL, or monitor and block the SQL, then based on that you need to decide how you can deploy the firewall – proxy mode, out-of-band, or host monitor.
- Deciding the Database Firewall policy that will help you define the multi-stage filtering rule for SQL traffic over the network. What rules you want, and when the rule is satisfied, what actions you want the database firewall to take.

3
Reports and Alerts

Oracle AVDF reports cover a wide range of activities including privileged user activity, changes to database schema, and SQL statements being executed. In addition, reports include information changes in database account management, roles and privileges, object management, stored procedure changes, and security configuration (Oracle Databases only).

Auditors access reports interactively through a web interface, or through PDF or XLS files. Report columns can be sorted, filtered, re-ordered, added, or removed. PDF and XLS reports can be scheduled to be generated automatically. Reports can also be defined to require signoff by multiple auditors. Users can use Oracle BI Publisher to create new or customize PDF and XLS report templates to meet specific compliance and security requirements. Furthermore, the Audit Vault Server repository schema is documented, enabling integration with third-party reporting solutions.

3.1 Types of Reports

The following are some of the reports available in Oracle AVDF.

Activity Reports

Activity reports track general database access activities such as audited SQL statements, application access and user logins. Specialized activity reports cover failed logins, user entitlements, before-after data modifications, changes to application tables, and database schema. For example, if we need to audit each time a user performs DDL SQL statements such as DROP or ALTER, the pre-built Database Schema report can display the data associated with that particular user and individual event details can be viewed.

Entitlement Reports

User Entitlement reports describe the types of access that users have in an Oracle Database, providing information about the users, roles, profiles, and privileges used. These reports are useful for finding duplicate privileges, and simplifying privilege grants. After an entitlement snapshot is generated, you can compare different snapshots to find how the entitlement information has changed over time. This is particularly useful for identifying any drift from an approved database entitlement baseline and can also pinpoint privilege escalations due to possible malicious activities.

Assessment Reports

Summarized risk findings help prioritize and guide immediate action on potential risks associated with your Oracle Database fleet. Assessment reports provide a fleet-wide simplified and centralized view of security configuration assessments for all your Oracle Databases, along with the security findings and associated risks.

You can expand on the risk of interest and continue to further analyze on the Assessment Report page with powerful interactive reporting. These reports can be available to the users and auditors responsible for all or a set of databases so that they can take appropriate action on the risk findings.

You can also define a security baseline and monitor deviations from your baseline security posture. The new Security Assessment Drift Reports can help you focus just on the newly introduced security configuration change.

Data Privacy Reports

You can import the sensitive objects in an Oracle database as a file, which could be generated by running the Database Security Assessment Tool (DBSAT) or Enterprise Manager (Application Data Model). Oracle AVDF will use this list to generate predefined reports such as activity on sensitive data, user's access rights to sensitive data, activity on sensitive data by privileged users, and others.

Stored Procedure and OS Correlation Reports

Stored Procedure Audit Reports can help keep track of the changes made to the stored procedures. Correlation Reports identify events on the database with the original Linux OS user for Oracle Database targets running on Linux. This is useful in cases where this user runs a shell or executes a command on the database as another user by using `su` or `sudo`.

Summary and Anomaly Reports

The report group contains Summary Reports, Trend Charts, and Anomaly Reports. These reports can be used to quickly review characteristics of user activity on specific targets or across the enterprise.

Summary Reports focus on statistical occurrence of various types of events generated by individual users or initiated from specific client IP addresses. Trend charts graphically present general event trends and also trends based on specific users, client IPs, and targets.

Reports could be used to identify anomalies such as new and dormant user and client IP anomalies over time. Activities by new users, or previously dormant users, can be an indication of account hijacking.

Compliance Reports

Standard default audit assessment reports are categorized to help meet regulations such as:

- General Data Protection Regulation (GDPR)
- Payment Card Industry Data Security Standard (PCI-DSS)
- Sarbanes-Oxley Act (SOX)
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Data Protection Act (DPA)
- IRS Publication 1075

3.2 Built-in Reports

There are many built-in reports that you can use to monitor your systems with Oracle Audit Vault and Database Firewall.

You can run the built-in report immediately, or you can create a schedule to run the report at a later date. You can specify a list of users who receive notifications of the report, or who need to attest to the report.

While browsing reports online, you can download them in HTML or CSV format. You can also schedule reports and download them in PDF or XLS format, or send them to other users. When you specify report notifications, you can use your own notification templates to send emails to other users with either a link to a report, or an attached PDF version of the report.

You can create customized reports based on the built-in reports and then save the new report formats to view them online. Oracle AVDF provides tools to filter, group, and highlight data, and define columns displayed in the reports.

Table 3-1 Available Types of Built-in Reports in Oracle Audit Vault and Database Firewall

Types of Reports	Description
Activity	A set of reports that track general database access activities such as audited SQL statements, application access activities, and user login activities. Some typical reports are: • Activity Overview: Displays information about all monitored and audited events. • Data Modification: Displays the details of audited data modifications for a specified period of time. • Data Modification Before-After Values: Displays the details of modified data and lists the values before and after modification. • Database Schema: Displays details of audited DDL activity for a specified period of time. • Failed Login Events: Displays details of audited failed user logins for a specified period of time.
Alert	Alert reports display the raised alerts and also let you respond online to alerts and notify others about them. Additionally, the generated alerts are available for analysis in the **Alerts** tab, where they can be filtered, and details pertaining to the event raising the alert can be viewed.
Assessment	These reports capture security assessment data from Oracle Databases and provide recommendations that help secure your Oracle Database system. It also includes drift reports against the baseline.
Stored Procedure Audit	A set of reports that help you keep track of the changes made to the stored procedures, such as stored procedure creation, modification, and deletion. The reports display details of audited stored procedure modifications for a specified period of time.
Compliance - Data Privacy Report (GDPR)	A set of reports that track possible violations that are defined by the following compliance areas: • Data Privacy Report (GDPT) • Payment Card Industry (PCI) • Gramm-Leach-Bliley Act (GLBA) • Health Insurance Portability and Accountability Act (HIPAA) • Sarbanes-Oxley Act (SOX) • Data Protection Act (DPA) • IRS Publication 1075

Table 3-1 (Cont.) Available Types of Built-in Reports in Oracle Audit Vault and Database Firewall

Types of Reports	Description
Database Firewall	For database Targets that you are monitoring with the database firewall, this set of reports gives detailed event information about SQL traffic. Much of the information is dependent on the firewall policy you have defined for the database. For example, you can see details of statements that had warnings, or were blocked, according to the policy. You can also see general information about SQL traffic to these databases, for example, statement type such as data definition and data manipulation. Some example reports are: • **Database Traffic Analysis by Client IP**: Displays audit details for statements by the protected database and client IP address. • **Database Traffic Analysis by OS User**: Displays audit details for statements grouped by protected database and OS user. The name of this report is **Monitored Activity by OS User** in Oracle AVDF 20.5 and later. • **Blocked Statements**: Displays audit details for blocked statements grouped by protected database and OS use. The name of this report is **Blocked Activity** in Oracle AVDF 20.5 and later.
User Entitlements	A set of reports that describe user access and privileges for Oracle Database targets, for example: • User Accounts: Displays information such as the target in which the user account was created or the user account name, and whether this account is locked or expired. • User Privileges: Displays information such as the target in which the privilege was created, user name, and privilege. • Object Privileges: Displays information such as the target in which the object was created, users granted the object privilege, and the schema owner. • Privileged Users: Displays information such as the target in which the privileged user account was created, user name, and privileges granted to the user.
User Correlation	For Oracle Database targets running on Linux, these reports let you correlate events on the database with the original Linux OS user. This is useful in cases where this user runs a shell or executes a command on the database as another user by using `su` or `sudo`.
Database Vault Activity	If your Oracle Database targets have Database Vault enabled, the Database Vault Activity report shows Database Vault events, which capture policy or rule violations, unauthorized access attempts, and other activity.

3.3 Custom Reports

There are two ways of creating custom reports with Oracle Audit Vault and Database Firewall. One way is to interactively customize the built-in reports by filtering data, and then save these interactive views so you can view them again online later.

The second way is to create your own reports by making simple customizations based on built-in report templates, or by using a software package such as Oracle BI Publisher. You can then upload your own custom reports into Oracle AVDF. This second method is discussed below.

For simple changes to the built-in report formats, you can also do some customizations without using a report authoring tool.

Oracle AVDF provides two types of files to help you get started creating custom reports. The first type of file is a report template in RTF format, which you can open in a tool such as Microsoft Word. The template determines the display of the report. For

example, you can easily add your own custom logo on the report. The second type of file is a report definition in XML format, which you can open in a text or XML editor. The report definition file specifies the data in the report.

You can download report definition and template files corresponding to any of the built-in reports, and then you can use these files as a starting point for creating your own custom report. Oracle AVDF documentation also provides information on event data collected from different types of targets that will help you create your own reports.

3.4 Alerts and Notifications

In many instances, you want to be notified as soon as certain events happen. Oracle AVDF lets you define rule-based alerts on audit records, whether these records come from the Audit Vault Agent or the Database Firewall. You can also specify notifications for those alerts. For example, you can set up an email to be automatically sent to a user, such as a security officer, or to a distribution list. Alerts can be also forwarded to syslog. This is useful if you want to integrate them with another system.

Because alerts are rule-based, if the rule definition is matched, then an alert is raised. For example, an alert can be defined which states that if user A fails to log in to database B after three tries, then an alert is raised.

Alert conditions are flexible and can include more than one event, and the events can come from different targets. The alert condition can also be a complex statement based on multiple fields in the collected audit data or SQL network event data. A good way to define an alert condition is to first look at the All Activity Report, which displays details of all captured audit events. From this report you can see possible events that may be of interest to you. Alerts can be threshold and time based as well. For example, if five login failures occur within one minute window, possibly indicating a brute force attack, then an alert can be raised.

3.5 Summary

Oracle Audit Vault and Database Firewall consolidates activity audit data from Oracle and non-Oracle databases, operating systems, and directories, and provides security and compliance reports. Through an accurate SQL grammar-based engine, the Database Firewall monitors SQL traffic and blocks unauthorized SQL. Now with modern and rich UI, and extensible monitoring platform, Oracle Audit Vault and Database Firewall 20 is your first line of defense with enterprise-level scale, security, and automation.

For more information, refer to the Oracle Audit Vault and Database Firewall documentation or the product data sheet, FAQ, and Technical Report.