ORACLE

Oracle Audit Vault and Database Firewall

Database Activity Monitoring and Security Posture Management for the Enterprise

SeptemberSeptember, 2023, Version 20.10

ORACLE

Purpose Statement

This technical paper provides an overview of Oracle Audit Vault and Database Firewall (AVDF), including a discussion of features, options, and use cases. It's intended to help you evaluate options for reducing security risk and improving regulatory compliance for your databases—including Oracle Database, Oracle MySQL, Microsoft SQL Server, PostgreSQL, IBM Db2, and SAP Sybase—with extension to support most other enterprise database platforms.

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this proprietary material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document is not part of your license agreement, nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described in this document remain at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

ORACLE

Table of Contents

ORACLE

List of Figures

List of Tables

Introduction

Oracle Databases contain more than half of the world's relational data. Much of that data is sensitive and has monetary value. That's why databases, especially Oracle Databases, are an attractive target for data thieves.

Database activity monitoring (DAM) is a database security technology that collects information from native database audit and network-based data capture to monitor and record database activity for analysis and reporting. Database activity monitoring is critical to securing data in a relational database, providing visibility into potentially malicious activity when preventive controls fail.

Combining audit data with network-based activity monitoring and blocking is the best way to gain a complete picture of database activity. Network monitoring alone can't catch all suspicious behavior; a solution focused solely on network monitoring won't understand database synonyms, function-based views, or stored-procedure activity. Conversely, 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 and help identify suspicious activity. The combination of auditing and network-based monitoring solves those issues and supports both security and regulatory compliance goals.

As the product's name implies, Oracle Audit Vault and Database Firewall (AVDF) contains a database firewall. Database firewalls monitor and evaluate incoming SQL commands at the network level, identifying and alerting on anomalies or out-of-policy operations. When appropriate, a database firewall can be used to block out-of-policy SQL from reaching the database at all.

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.

AVDF was first introduced in 2012, merging two existing products—Oracle Audit Vault and Oracle Database Firewall—into a single unified offering that, for the first time, took advantage of the synergy between native database audit and network-based activity monitoring to provide a comprehensive view of database activity. AVDF 20.9 expands the product's capabilities from database activity monitoring (DAM) to database security posture management (DSPM).

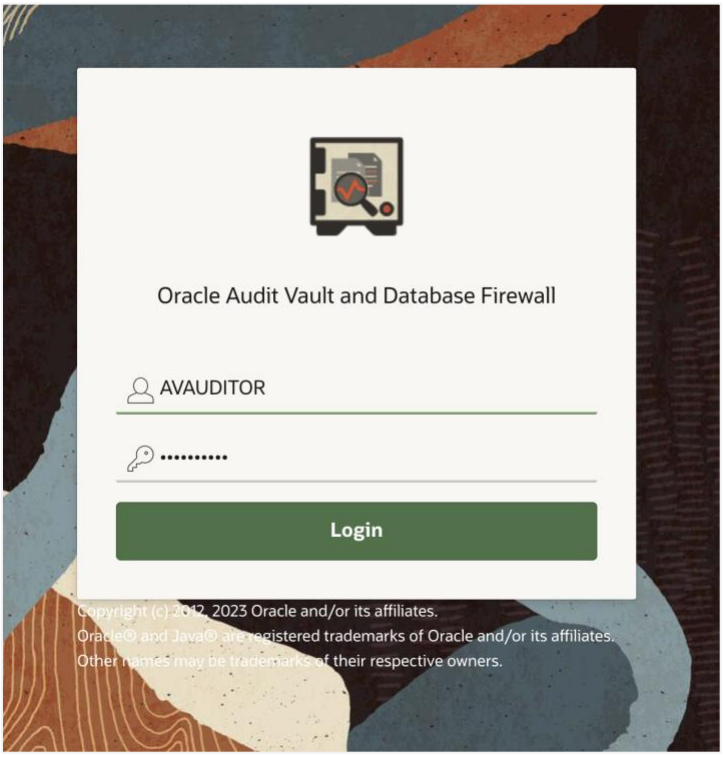

Figure 1. Oracle Audit Vault and Database Firewall Login Page

Oracle Audit Vault and Database Firewall Overview

Oracle Audit Vault and Database Firewall (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.

AVDF aggregates user audit data from Oracle and non-Oracle databases, operating systems (OSs), and directories, whether in the cloud or on premises, into a single repository for analysis, alerting, and reporting. AVDF is an enterprise-level audit platform with scalability, security, and automation. AVDF also monitors SQL statements submitted to the database over the network and can examine, allow, log, and even block unauthorized SQL statements. The Database Firewall offers network-based SQL inspection with easy rules to identify anomalies and block unauthorized SQL or SQL injection attacks.

Through powerful reporting and alerting, AVDF supports compliance audits and incident investigations and provides a modern, scalable platform for a full 360-degree view. AVDF includes extensive reporting capabilities by using a simple filter-based interactive reporting interface that allows quick access to relevant information. With AVDF, a single system can monitor activity across thousands of databases, providing a single console from which to report and analyze security events throughout the database estate, including supporting infrastructure.

AVDF supports database activity monitoring for common enterprise-class databases. Out-of-box audit collection support includes Oracle Database, Oracle MySQL, Microsoft SQL Server, SAP Sybase, IBM Db2 LUW, and PostgreSQL. Support for most other databases and applications is possible by using the included custom connector framework, which collects data through JDBC or RESTful API. The custom collection is also possible from systems that write audit data to XML or JSON files. A Java-based software development kit (SDK) is included to accommodate those rare targets that can't be accessed by using any custom connector framework options. Database Security Posture Management is currently only provided for Oracle Database.

AVDF's fleet-level view facilitates insight into Oracle Database configuration, enabling the detection of issues across the database estate. Armed with this information, administrators can quickly mitigate issues to reduce risk and control data exposure.

Key Features of Audit Vault and Database Firewall

AVDF is the culmination of over a decade of continuous development. AVDF offers a simplified user interface, extended coverage for all popular databases, a scalable and robust underlying infrastructure, a scalable and proven architecture for collecting before and after values, and more.

User Interface

AVDF's user interface engine gives you a modern, responsive, intuitive look and feel. The UI is simplified and optimized for common workflows and easier navigation. The audit vault server and the database firewall are managed from the same console, which centralizes administrative activities and reduces the number of consoles that need monitoring.

Coverage for Most Database Types

AVDF supports audit and network collection for Oracle Database, Oracle MySQL, Microsoft SQL Server, SAP Sybase, and IBM Db2 LUW. Audit collection is also supported for PostgreSQL and MongoDB databases. The custom collector framework lets you add audit collection for other databases that produce audit data in XML, JSON, or CSV format, or write their audit trails to a database table that can be accessed through JDBC.

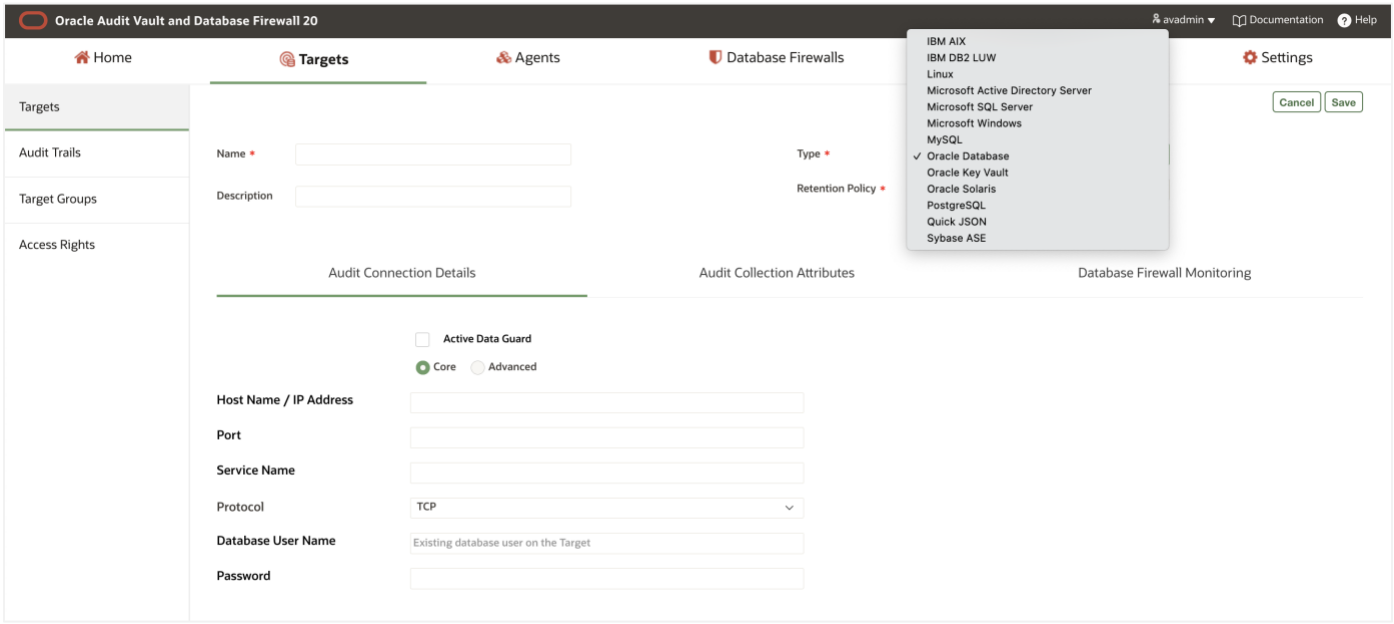

Figure 2. Registering a New Target

Database Security Posture Management

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.

You can start by understanding the high and medium risks, then look at the advisory and evaluate categories to further harden your security posture. Expand on the risk of interest and continue to further analysis on the Assessment Report page with powerful interactive reporting provided by AVDF. With DSPM, you can define a security baseline and monitor deviations

from your baseline security posture. The security assessment drift reports can help you focus just on the newly introduced security configuration changes.

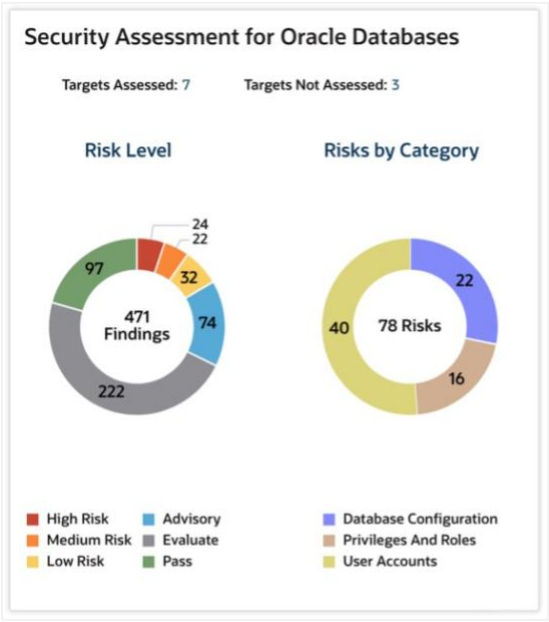

Figure 3. Security Assessment for Oracle Databases

Before-and-After Value Collection

Before-and-after value collection is just what it sounds like. If a data value changes, AVDF records the old value (*before* the change) and the new value (*after* the change), along with who made the change and when the change was made. Before-and-after value collection is extensively used in the healthcare and financial services and in many other regulated industries. With before-and-after value collection, auditors can track the life cycle of individual data attributes throughout changes—an essential component of many data governance mandates.

AVDF uses Oracle GoldenGate for before-and-after value collection. (Restricted use of GoldenGate is included with AVDF; see the AVDF License Information guide for details.) Using GoldenGate brings many advantages, including improved throughput, easier administration, support for multitenant databases, and support for Oracle and non-Oracle databases. AVDF 20.9 has extended the ability to capture before-and-after values to Microsoft SQL Server. This new functionality helps organizations improve their compliance reporting and enables them to monitor critical data elements throughout the data life cycle.

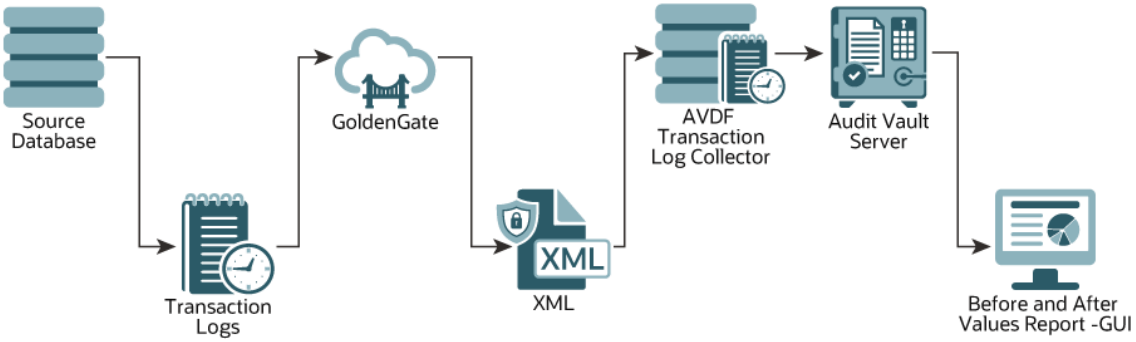

Figure 4. Transaction Audit Trail Data Flow

Improved Operations Experience

AVDF supports automated archiving of collected data, integration of AVDF users with Microsoft Active Directory or OpenLDAP, multipath fiber channel, network interface card bonding, and AVDF port customization. AVDF administrators and systems integrators will find it easy to work with and a good fit for modern data centers and cloud deployments.

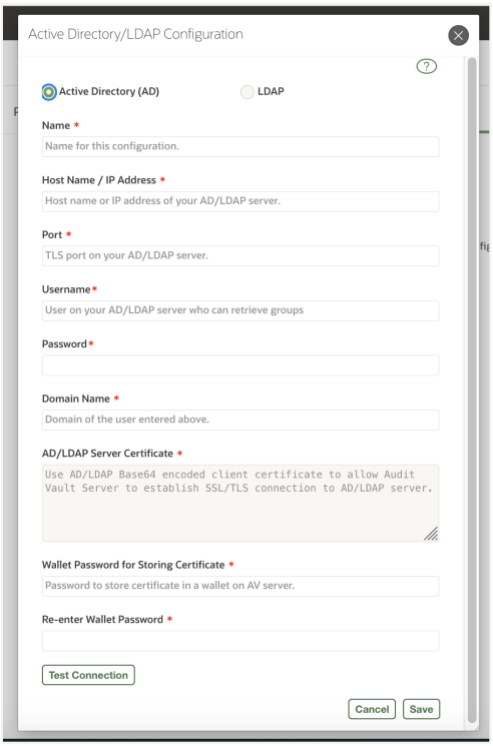

Figure 5. Active Directory Integration

Reports and Alerts

Reports and alerts are the primary output of a DAM system like AVDF. Information collected by the system is presented in the form of reports and, when appropriate, alerts.

Alerts notify interested parties when conditions that rate immediate attention are detected. Common alerts include multiple failed logins in a short time or unauthorized attempts to access sensitive data. In AVDF, alerts can be triggered based on individual events like someone attempting to access a highly sensitive date or event trends like more than 10 failed login attempts from a single IP address over the course of one minute.

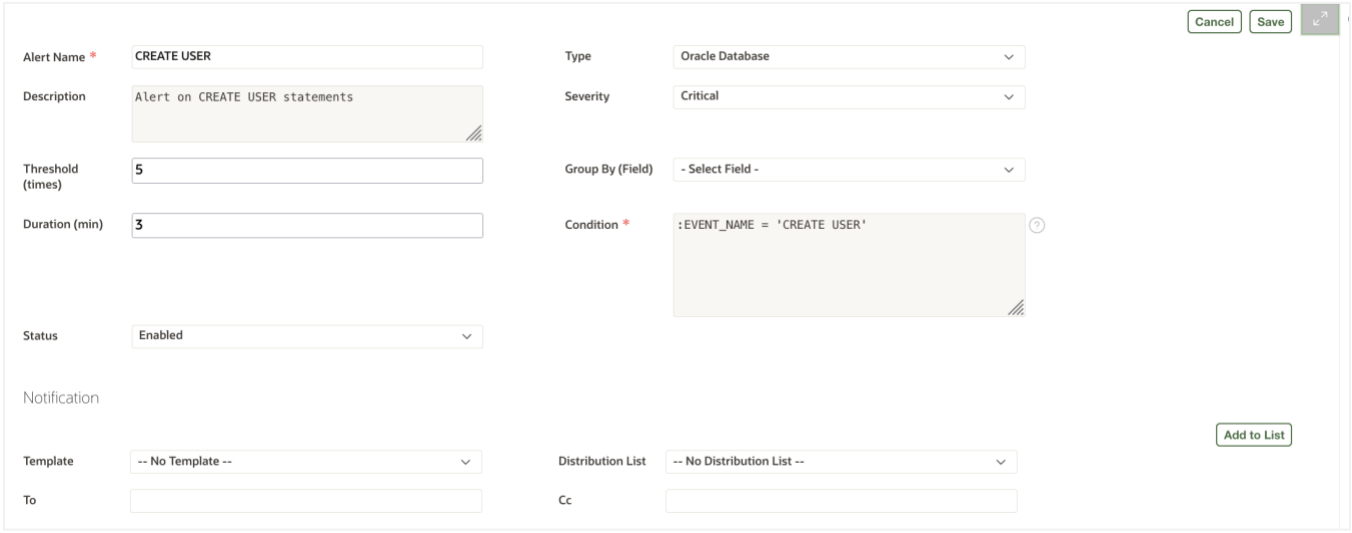

Figure 6. Creating an Alert Policy

Reports can be formal reports for record or regulatory purposes, or ad hoc interactive reports that support investigations. Auditors can access reports through the AVDF console, or reports can be scheduled for automatic generation in a spreadsheet or document format and distributed through email. If needed, an attestation that a report has been reviewed, along with any notes from the reviewer, can be tracked within AVDF.

AVDF comes preconfigured with dozens of reports ready to run—from compliance reports supporting regulations like HIPAA, PCI, and GDPR to standard security requirements like failed login reports, SUDO activity reports, and DML. Custom reports can be easily created and preserved for later use.

The Audit Insights dashboard offers a comprehensive view and provides immediate insight into the top user activities across one or multiple databases.

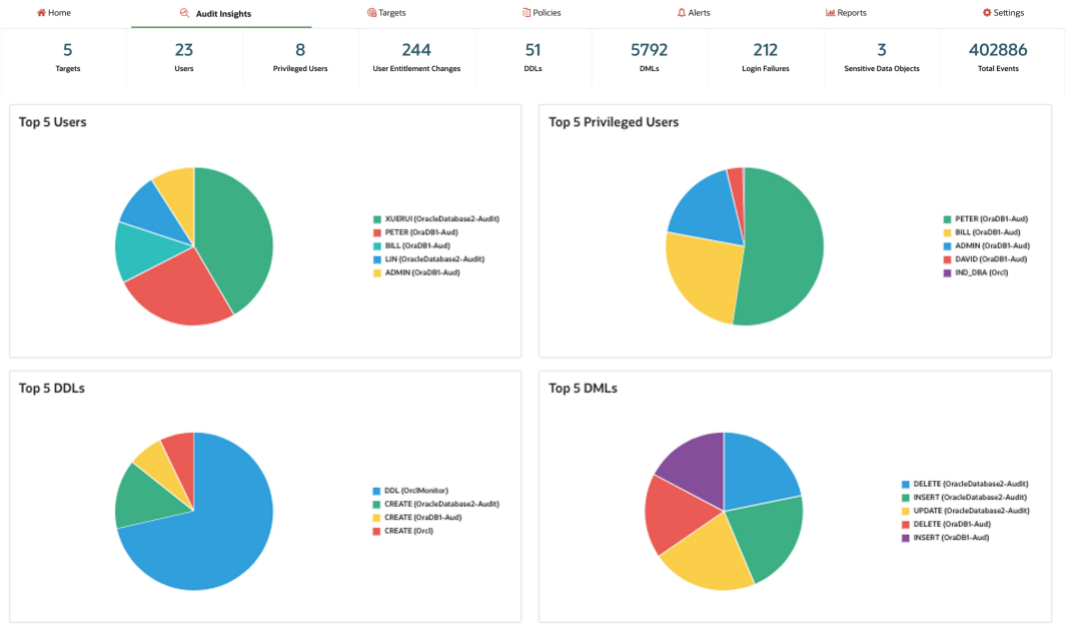

Figure 7. Audit Insights Dashboard

In addition to its extensive reporting capabilities, AVDF also allows the use of external reporting or analytics tools that are compatible with Oracle Database, and a limited-use license for Oracle Business Intelligence Publisher is included with AVDF.

Audit Vault and Database Firewall Components

AVDF provides a comprehensive and flexible solution for monitoring and protecting database systems. AVDF is composed of the following primary components:

- Audit vault server
- Audit vault agent
- Database firewall
- Host monitor

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 OS
- Oracle Database, which serves as the audit repository.
- The AVDF application, which provides the interface for the AVDF console and the AVCLI command-line interface

AVDF consolidates data from *audit targets,* including Oracle and non-Oracle databases, OSs, directories, file systems, and application-specific audit data. This data is collected from audit targets and loaded into the audit repository, which is the Oracle Database that resides on the audit vault server.

The audit repository database is encrypted (using Oracle Transparent Data Encryption) and protected with Oracle Database Vault.

Audit Vault Agent

An audit vault agent retrieves audit data from audit targets and securely forwards that data to the audit vault server. A single audit vault agent can collect data from multiple targets and audit trails. The audit vault agent is lightweight, consuming little in the way of CPU, memory, or disk space. Communications between the audit vault agent and the audit vault server use TLS 1.2.

AVDF 20.9 introduces an “agentless” collection of unified audit data in Oracle Databases. With the agentless collection, you use the agentless collection service that comes with the audit vault server instead of deploying the audit vault agent on the target host machines. The agentless collection service is automatically installed when you install the audit vault server or when you update AVDF to release 20.9 or later. In addition to Oracle Database, you can now collect audit data from Microsoft SQL Server in an agentless mode or a remote host without installing any agent on target machines from 20.10 onwards.

Database Firewall

The database firewall monitors network activity sent to the database and examines SQL statements before they reach the database. A database firewall policy governs what is done with those SQL statements—the database firewall might pass them on to the database without further action, or it might forward information about them to the audit vault server for entry into the audit repository. If the database firewall is configured in line with that traffic (acting as a database proxy server), then the firewall can also block SQL statements from ever reaching the target database or substitute a replacement SQL command for the blocked statement.

The database firewall uses a multiple-stage policy to determine what to do with an SQL statement.

- In the first stage, the policies examine the originating connection’s IP address, OS username, the program being used to connect to the database, and the database account being used for the connection. The firewall can be configured to

allow connections that meet conditions based on these factors, log them for later examination, or (if in line) block them.

- The next stage is based on the SQL statement's structure, with pass, log, or block actions based on the statement's syntax. This type of policy is an excellent way to block or alert SQL injection attacks.
- The third stage is based on the tables and views being accessed and the operations being performed (for example, insert, update, or delete).
- The fourth stage is the anomaly stage; any SQL statement not handled in any of the previous stages is handled by this policy. You can think of it as the "else" phrase in a case statement. Any SQL statement that reaches the fourth stage is passed, logged, or blocked depending on the settings in this portion of the firewall policy.

We introduced global sets in 20.9 to support database firewall customers with the same set of privileged users across multiple database targets, and instead of repeating the list for every database, customers want to use that same set across database firewall policies. Now we have enhanced the global sets feature of database firewall policies and extended it to session context information, including IP address, OS user, client program, and database user. These global sets are usable across multiple database firewall policies, simplifying database firewall policy management.

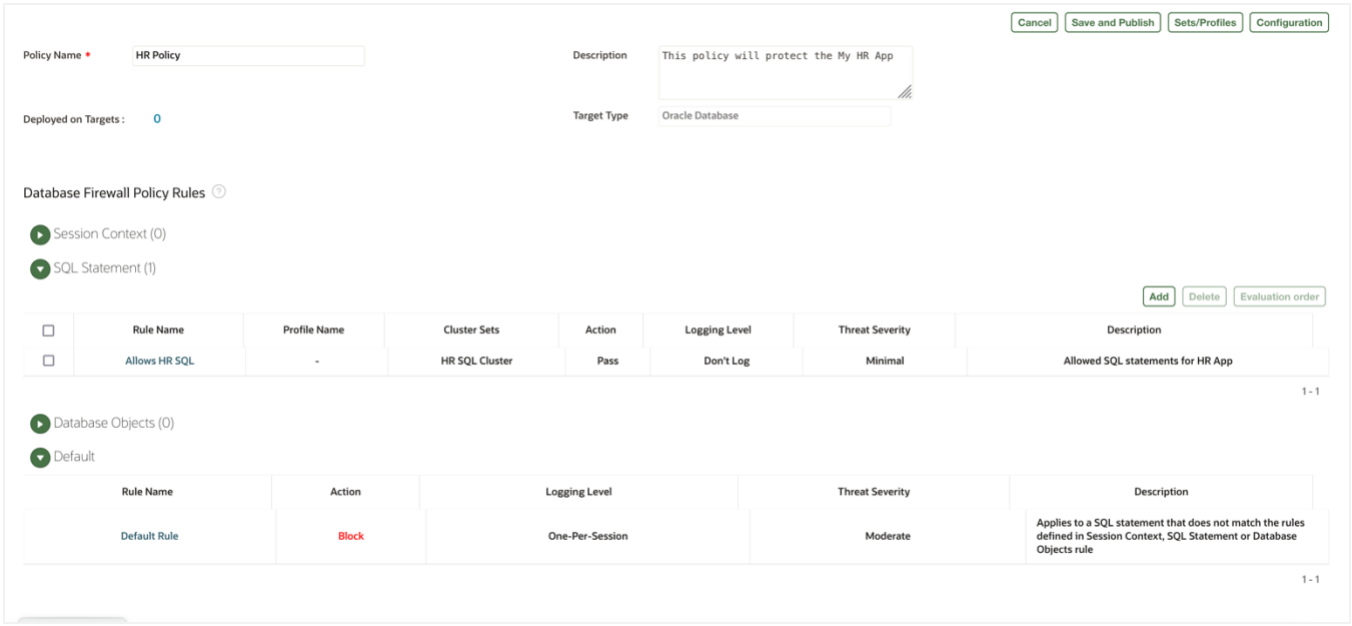

Figure 8. Database Firewall Policies

Host Monitor

Host monitors are remote sensors for the database firewall. A host monitor is installed on the same server as the audit target and monitors incoming network traffic for the database. Host monitors only monitor traffic; they don't block traffic. Anything captured by the host monitor is forwarded to the database firewall for analysis according to the target's policy on that firewall, with logged SQL statements forwarded to the audit vault server for insertion into the audit repository.

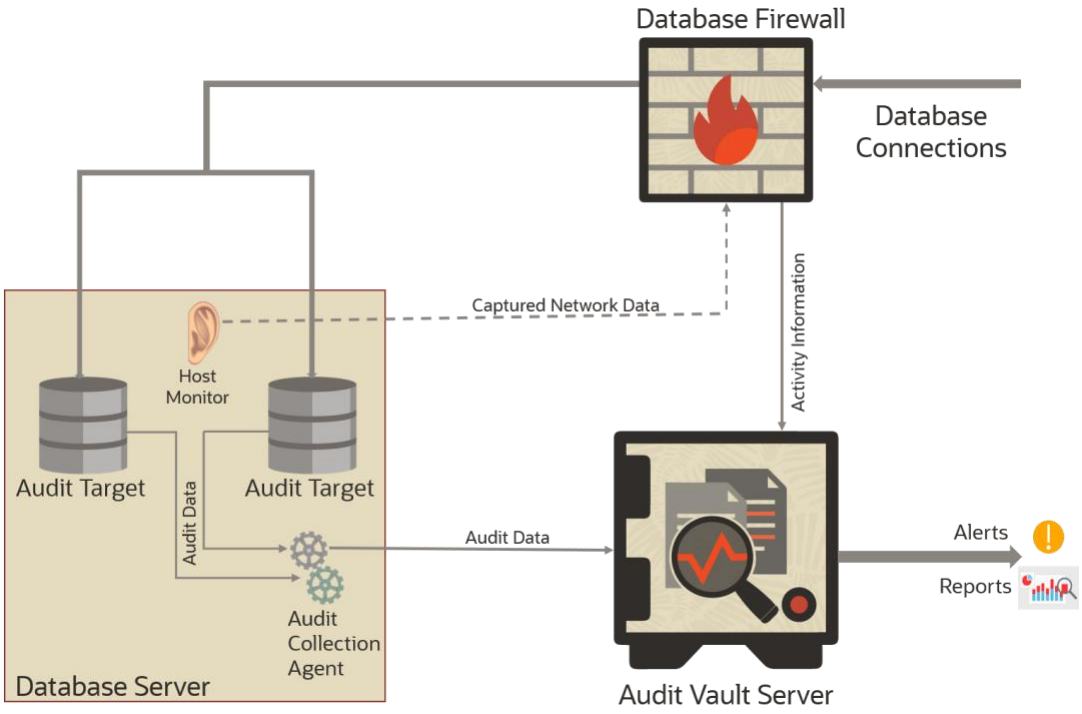

Figure 9. Simplified Architecture Diagram

Scalability and Security

Audit data is an important record of business activity, and it must be protected against modification to ensure the integrity of reports and investigations. AVDF stores audit data in a secure repository built using Oracle's industry-leading database technology. To prevent unauthorized access or tampering, audit and event data is encrypted at every stage, in transit, and at rest. Timely transfer of audit data from source systems to the audit vault server is critical to close the window on intruders who might attempt to modify audit data and cover their tracks.

AVDF supports two broad categories of users: auditors and administrators.

- Auditors configure auditing and monitoring policies and define, generate, and access audit reports and alerts.
- Administrators configure basic network and host settings for the secured targets, start and stop audit vault agents and database firewalls, and configure and monitor audit vault server operation. Administrators don't have access to audit information.

Within the two role categories, further separation of duties can be defined. A subset of databases can be assigned to individual auditors and administrators, ensuring that a single repository can be deployed to support an entire enterprise spanning multiple organizations, subsidiaries, or geographic regions. Fine-grained authorizations are particularly important when information spans multiple countries with different privacy regulations and data protection requirements.

The repository is built on an embedded Oracle Enterprise Edition Database that includes numerous Oracle technologies, including compression, in-memory optimization, partitioning, encryption, and privileged user controls. The use of compression is particularly important for the optimized storage of consolidated data. The combination of these technologies and Oracle Database results in a repository with massive scalability, high availability, and security.

A single instance of AVDF can scale to support thousands of databases. The only limit is the capability of the server hardware where the audit vault server is installed.

Flexible Deployment Options

AVDF is flexible enough to meet almost any deployment scenario.

Audit Vault Agents

Audit vault agents are typically installed on the same server as the audit target. In some cases, however, agents can be used to retrieve audit data from a remote audit target—for example, from databases where the audit volume is low, or when it's not practical to install an agent on the database server. As mentioned earlier, Oracle Database targets can take advantage of agentless collection from AVDF 20.9 onwards, and Microsoft SQL Server databases can use it from 20.10 onwards.

Database Firewall

Database firewall can monitor network traffic to the database in the following ways:

- The database firewall can be placed in line with the network traffic, acting as a proxy server between the database and database clients. This deployment mode is common in virtualized environments or cloud-based environments, in which control over the network is limited. The database firewall can block traffic only when it's placed in line with the network traffic flowing to the database, so this deployment model is always used when blocking is required.
- The database firewall can be positioned out-of-band with the network traffic, with traffic destined for the database server copied to the database using a network SPAN port, a network tap, or a network packet replicator. As long as the database firewall can "see" the SQL statements flowing to the database, and the database's response to those statements, the technology used doesn't matter. This deployment model is most often used for on-premises deployments in which blocking isn't required.

Host Monitor

When it's impractical to either route traffic through or copy traffic to the database firewall, a host monitor can be used. Host monitors capture network activity at the database server and forward that activity to the database firewall for analysis. Host monitors are another common deployment option in virtualized environments.

Capabilities

All of the database firewall deployment modes allow for monitoring activity. Only the inline proxy allows blocking.

Table 1. Database Firewall Deployment Modes

Deployment Mode	Details	Monitoring?	Blocking?
Inline proxy	All client connections go through a firewall, including return traffic.	Yes	Yes
Host monitor	The agent running on the database host listens to incoming traffic.	Yes	No
Out-of-band	Database traffic sent to it by a SPAN port or packet replicator is monitored.	Yes	No

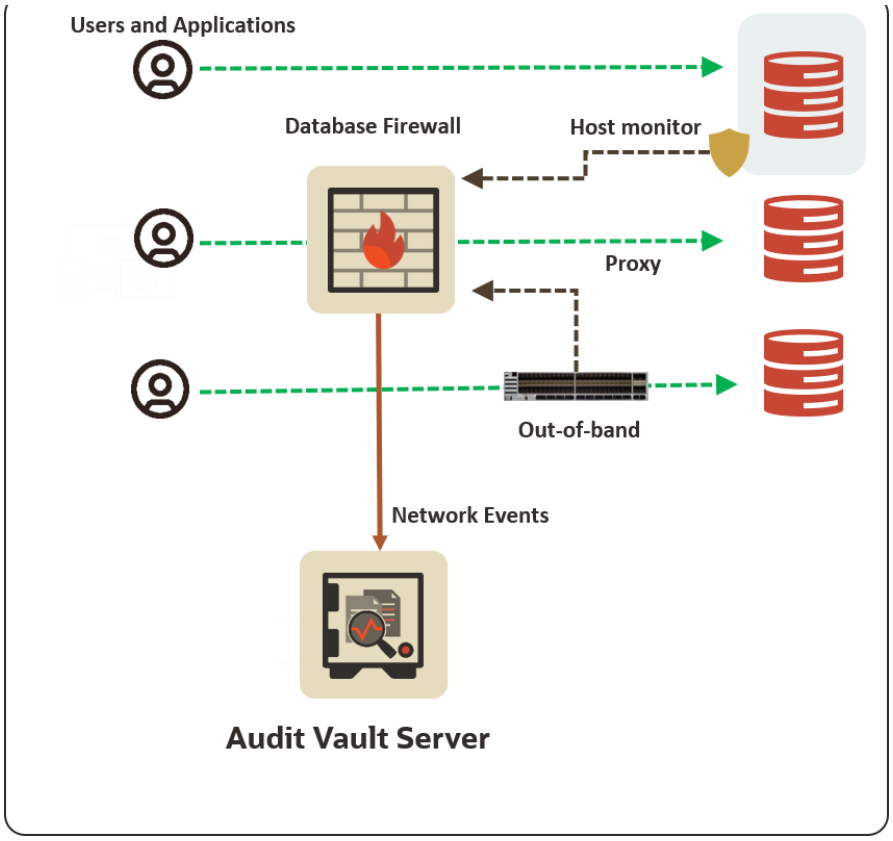

Figure 10. Database Firewall Deployment Options

High Availability

Both the audit vault server and the database firewall can be configured in pairs to provide a high-availability (HA) system architecture. These paired servers are known as *resilient pairs*.

Audit Vault Server HA

When configured as a resilient pair, the audit vault server has a primary server, which performs all server functions, and a secondary server, which is synchronized with the primary by using Oracle Data Guard. If the primary audit vault server fails, the secondary server automatically comes online, and both audit vault agents and database firewalls begin sending their data to the secondary server.

Database Firewall HA

There are two forms of database firewall HA. Which one is used depends on whether the database firewall is being used in one of the monitoring-only configurations or in proxy mode.

Database Firewall and HA in an Out-of-Band or Host Monitor Configuration

In monitoring mode, the database firewall is configured as a resilient pair, with configuration for both synchronized by the audit vault server. There is no communication between the primary and secondary database firewall; they act independently of each other. The primary and secondary database firewalls receive the same traffic, and both send their logs to the audit vault server. The audit vault server processes logs only from the primary, ignoring and discarding logs from the secondary until the primary becomes unavailable.

Database Firewall and HA in a Proxy Configuration

When a database firewall is used in a proxy configuration, two or more database firewalls can be used to achieve the necessary level of fault tolerance.

Traffic might be directed to the database firewalls from a load balancer, by DNS, or by using client-based configurations like load-balance or transparent application failover.

All firewalls in the configuration are online (there is no concept of a primary and a standby for inline), and the audit vault server processes logs from all the database firewalls.

Integration with Third-Party Solutions

AVDF can integrate with third-party security solutions like a SIEM, Splunk, or log aggregator either by *pushing* data to them or by allowing the third-party solution to *pull* data directly from the audit repository.

Data is *pushed* to a third party by sending alerts via syslog. The content and the format of these alert messages are fully customizable. Auditors can define an unlimited number of message templates and apply them to different alert definitions.

Third-party solutions can *pull* data from AVDF by connecting directly to the audit repository to extract audit data for further analysis and correlation with other data feeds. Third-party access to audit data is controlled by the same privilege model used for AVDF auditors, so it's possible to provide access to only certain subsets of audit information.

Conclusion

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. Extensive reporting and alerting capabilities provide auditors and security personnel with access to detailed information and early warning alerts on potential malicious activity. Sources beyond databases can be monitored, with ready-to-use support for the consolidation of audit data from various OSs and directory services. An extensible plug-in architecture enables custom audit sources to be added to the collection framework, enabling application-specific audit data to be aggregated and reported together with other event data in the repository. AVDF delivers effective detective and preventive controls for Oracle and non-Oracle databases alike.

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

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle