Oracle Audit Vault and Database Firewall 20

Frequently Asked Questions

May 2022

PURPOSE

This technical report answers some of the most commonly asked questions about Oracle Audit Vault and Database Firewall 20.

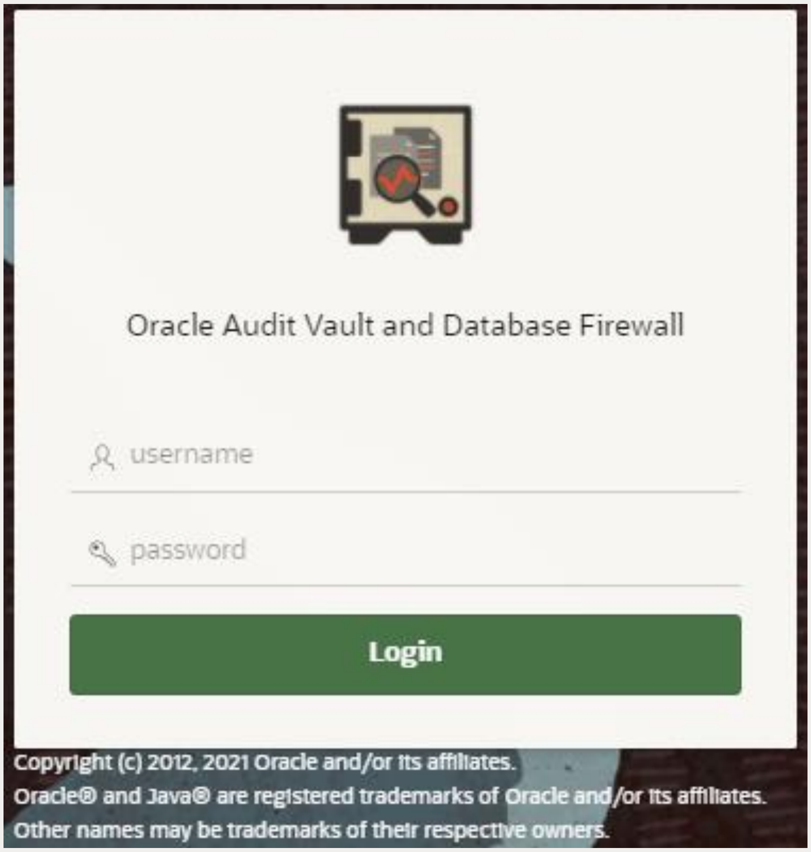
INTENDED AUDIENCE

If you are responsible for designing, implementing, maintaining, or operating security controls for an enterprise database, this paper is intended for you.

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 confidential 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 to implement and upgrade the product features described. It is not a commitment to deliver any material, code, or functionality and should not be relied upon in purchasing decisions. The development, release, and timing of any features or functionality described in this document remain at the sole discretion of Oracle.



Oracle Audit Vault and Database Firewall

Copyright (c) 2012, 2021 Oracle and/or its affiliates.
Oracle® and Java® are registered trademarks of Oracle and/or its affiliates.
Other names may be trademarks of their respective owners.

Figure 1: AVDF Login Page

1. PRODUCT OVERVIEW

a. What's new in Oracle Audit Vault and Database Firewall (AVDF)?

Oracle AVDF 20 has a revamped; modern user interface with simplified navigation for common workflows, expanded audit collection for new target types (PostgreSQL, MongoDB using a simple attribute mapping table), a simplified firewall, and additional features for enterprise support. Refer to the Oracle AVDF 20 Release Notes for a complete feature list.

b. How are Audit Vault and Database Firewall related? Do I need both of them?

Oracle AVDF supports native audit collection and network-based SQL traffic monitoring. Audit data is stored in the Oracle Audit Vault Server and the network events from the Database Firewall. This allows you to correlate the activity data and create reports.

Oracle recommends a holistic approach and supports database auditing and network-based SQL traffic monitoring. You can start with either capability and expand your architecture to include both if needed.

c. Which target types and versions are supported by Oracle AVDF?

Oracle AVDF supports Oracle Database, Microsoft SQL Server, MySQL, IBM Db2, PostgreSQL, SAP Sybase, and operating system logs for Linux, Windows, Solaris, and AIX. Data from application audit tables, XML, CSV, JSON, and MongoDB can be collected using custom collectors. For details, see the Platform Support Matrix in the Oracle AVDF 20 Installation Guide.

d. How does Oracle AVDF consolidate audit data from other sources such as applications?

Oracle AVDF can collect audit data from application tables or files (XML, JSON, CSV), map them to the standard format, and include them in a single report across all sources. For details, refer to the Oracle AVDF Developers Guide.

e. What is the difference between auditing and network monitoring? Do I need both?

Auditing typically captures detailed information after a certain event, whether from a SQL statement directly or through a stored procedure call. Monitoring SQL traffic helps you analyze and take action on the SQL statement before it reaches the database, making it possible to block suspicious statements. In both cases, you can specify the conditions under which you want to collect the audit or the event logs. Both give different views on the same event, one after and one before. Alerts can be raised on both of them.

Oracle recommends a holistic approach and supports database auditing and network-based SQL traffic monitoring. Customers can start with either capability and expand their architecture to include both.

f. How do I provision auditing and database firewall policies?

Oracle AVDF provides an interface to view your audit policies and, with a single click, provision them in the target database. Firewall policies can also be configured in the UI to allow, log, alert, substitute, or block the SQL. In addition, firewall policies can be configured for Oracle databases to capture the returned number of rows from a SQL SELECT statement and used for monitoring and alerting data exfiltration attempts. For more information, refer to the Auditor's Guide.

g. What are the different ways to monitor database traffic?

You can configure the Database Firewall for monitoring and blocking or only for monitoring. To implement monitoring and blocking, you must configure the firewall in proxy mode, where all database traffic is routed via the firewall. To implement network-based SQL traffic monitoring, you can have the span port of network switches send the traffic to the database firewall, or you can set up the host monitor on the database machines to forward the SQL traffic to the Database Firewall. For details, refer to the Administrator's Guide.

h. Can I get a unified report with both audit data and network logs?

Audit Vault Server consolidates your audit data and network SQL traffic to provide a unified view of all database activity from the audit logs or captured SQL traffic. Alerts and reports are created from the consolidated data.

i. Can I correlate OS activity with the database activities to get the full picture?

Yes, Oracle AVDF provides a report that displays details of database events correlated with the original Linux OS user before the SU or SUDO transition.

2. KEY USE CASES

a. How does Oracle AVDF help meet compliance reporting requirements?

Oracle AVDF provides pre-built compliance reports for GDPR, PCI, GLBA, HIPAA, IRS 1075, SOX, and UK DPA. For example, under GDPR compliance, we provide reports on who has access to your sensitive data and who is accessing your sensitive data. You can customize the reports to meet your specific objectives or industry/region-specific compliance requirements. Third-party reporting tools can also connect to the Audit Vault schema for analysis and reports.

b. Can Oracle AVDF audit and track privileged users' activities?

You can enable audit policies for admin activity and name users. Oracle AVDF has pre-defined reports, including privileged user reports, which show all audited activity by privileged users.

c. Can Oracle AVDF track access to sensitive data in databases?

You can import the sensitive object list as a file, which could be generated by running the Oracle Database Security Assessment Tool (DBSAT) or Enterprise Manager (Application Data Model). Oracle AVDF will use this list to generate pre-defined reports such as activity on sensitive data, activity on sensitive data by privileged users, etc.

d. How does Oracle AVDF help in investigating misuse or unauthorized access?

Oracle AVDF users can use the "All Activity Report" to analyze which objects were accessed. Oracle AVDF can filter by user, object, dates, etc., and analyze the resulting data to see if unauthorized users access the objects. Additionally, for Oracle databases, users can use the returned rows from SQL SELECT statements to investigate data exfiltration attempts.

e. Can Oracle AVDF help in tracking changes to users, roles, privileges, and entitlements?

Oracle AVDF can be configured to check entitlements for Oracle Databases on a scheduled basis and provide differential reporting on what has changed since the last report. Oracle AVDF identifies changes to users, roles, and privileges.

f. How does reporting before/after values help security and compliance?

Corporate security policies and regulations such as HIPAA require that changes made to sensitive data are audited and that the before and after values of the record are captured. Oracle AVDF captures the before/after values using the Oracle GoldenGate Integrated Extract process (restricted license included) and makes those available in the Oracle AVDF reports for analysis. See Oracle AVDF Administrators Guide and Auditors Guide for details.

g. How does Oracle AVDF help with Database Activity Monitoring (DAM) and SIM/SIEM initiatives in my organization?

Oracle AVDF is a DAM solution providing native audit data collection and network-based SQL traffic monitoring. Oracle AVDF supports alerts, reports, and audit data archival. Oracle AVDF can send events to Syslog for integration with SIEM systems. Oracle AVDF schema is open and can be queried.

3 SECURITY

a. Does Oracle Database Firewall monitor encrypted traffic to the targets?

Database Firewall can monitor the traffic to and from an Oracle Database when Oracle Native Network Encryption is used. For non-Oracle databases and for Oracle Databases that use TLS network encryption, the Database Firewall cannot interpret this SQL traffic. You can use SSL or TLS termination solutions to terminate the SQL traffic just before it reaches the Database Firewall so it can interpret the SQL traffic and enforce the policies.

b. How is the data stored in Oracle AVDF secured?

Oracle AVDF encrypts collected data using Transparent Data Encryption and encrypts the network traffic from the targets. Oracle AVDF provides separation of duties between the administrator and the auditor and uses Database Vault to restrict access to data. See the General Security Guidelines in the Oracle AVDF Administrator's Guide for details.

c. Can Oracle AVDF work with Active Directory for authentication?

Oracle AVDF 20 supports Active Directory integration for user authentication. You can also create Oracle AVDF admins/auditors as Active Directory users. For details, see the Oracle AVDF Administrator's Guide.

4. ENTERPRISE CAPABILITIES

a. How does Oracle AVDF scale with high targets or a high volume of audit/log data?

When configured per the sizing guidance, an Audit Vault Server can support audit and firewall event data collection up to 1000 audit trails, and each agent can support up to 20 audit trails. For sizing guidance, refer to "Audit Vault and Database Firewall Best Practices and Sizing Calculator" (MOS Note: 2092683.1) - you can size the CPU, memory, and disk needed for the Audit Vault Server, Agent, and Database Firewall based on your environment. You will need to provide the number of targets, average audit data generated per day, retention period, number of firewall targets, etc., to generate the sizing guidance.

b. Can Oracle AVDF handle the high load from Oracle Exadata, clustered databases, etc.?

Oracle AVDF can scale to support audit data collection from Oracle Exadata and other clustered databases. You can configure the number of agents based on the total targets and expected audit ingestion rate. In Oracle AVDF 20.5 (and later), the Audit Vault Agents automatically choose the best possible configuration for improving the audit collection rate. This dynamic multi-threaded collector functionality effectively utilizes the resources of the Audit Vault Server and Audit Vault Agent. For details, see Registering Targets in the Administrator's Guide.

c. Does Oracle AVDF support cloud targets in addition to on-premises targets?

Oracle AVDF can monitor targets deployed on-premises and on the Oracle Cloud, including Oracle Autonomous Database services. Audit Vault Server collects data for traditional audit trails, fine-grained audit, Database Vault audit, and Unified Audit from audit trails on cloud or on-premises databases. Refer to the “Oracle Audit Vault And Database Firewall Hybrid Cloud Deployment” chapter in the Administrator's Guide for details.

d. How does Oracle AVDF support high availability for fault tolerance?

Oracle AVDF supports high availability configuration for Audit Vault Servers and Database Firewall, whereby the standby server becomes the primary in the event of an outage. In addition, Oracle AVDF agents can be configured with multiple IP addresses, enabling them to be run on a machine with multiple NICs or on different machines and managed by a third-party cluster management software. Refer to the Administrator's Guide for details.

e. Can Oracle AVDF archive audit/log data to meet retention requirements from regulations?

Audit Vault Server supports data retention policies on a per-target basis, making it possible to meet internal or external compliance requirements. Audit data can be automatically archived in a low-cost external repository and retrieved as per the target-specific policy. Refer to the Administrator's Guide for details.

f. Can Oracle AVDF raise alerts on anomalous activity to minimize analysis time?

Oracle AVDF has a powerful alert builder that configures alerts on the collected audit and firewall data based on various conditions. Oracle AVDF can display the alert on the dashboard, send it as an email, or send it to Syslog.

g. How is Oracle AVDF integrated with Oracle security products such as Oracle Key Vault, Oracle Database Vault, and Oracle Database Security Assessment Tool (DBSAT)?

The output of the Oracle DBSAT containing the list of sensitive columns/tables in your schema can be imported into Oracle AVDF, and audit activity on these tables can be viewed in the Oracle AVDF Reports. Oracle AVDF can read audit data from the Database Vault audit trail and display it in the Oracle AVDF Reports. Oracle Key Vault can be added as a target in Oracle AVDF. Oracle AVDF will collect audit data from Oracle Key Vault and generate all activity reports in Oracle AVDF.

h. Can an Oracle enterprise manager manage Oracle AVDF?

Oracle AVDF plug-in provides an interface within Oracle Enterprise Manager Cloud Control for administrators to manage and monitor Oracle AVDF components. Refer to System Monitoring Plug-in User's Guide for Audit Vault and Database Firewall for complete information. Refer to Compatibility with Oracle Enterprise Manager to check the supported versions of Oracle Enterprise Manager with Oracle AVDF 20.

5. DEPLOYMENT

a. What type of hardware or VMs can I run Oracle AVDF on? How do I size them?

Any Intel x86 64-bit hardware platform supported by Oracle Linux release 7 can be used to deploy the Oracle AVDF components. Please refer to the Hardware Certification List for a complete list of certified hardware. Each Audit Vault Server and Database Firewall must be installed on its dedicated x86 64-bit server. Please refer to the 2.2.1 Product Compatibility Matrix in the Installation Guide.

Oracle AVDF is also deployable in the Oracle Cloud Infrastructure (OCI) from the Oracle Cloud Marketplace. With the marketplace image, it's possible to deploy a fully functioning Oracle AVDF system within a few minutes. Oracle Cloud offers the flexibility to scale up compute resources to meet growing requirements. Ease of scaling up gives the option to start with a small VM shape and scale up as workload increases.

For sizing guidance, refer to "Audit Vault and Database Firewall Best Practices and Sizing Calculator" (MOS Note: 2092683.1) - you can size the CPU, memory, and disk needed for the Audit Vault Server, Agent, and Database Firewall based on your environment. You will need to provide the number of targets, average audit data generated per day, retention period, number of firewall targets, etc., to generate the sizing guidance.

Although Oracle AVDF can be run on virtualized environments such as Oracle VM Server or VMware, we recommend installing it on physical hardware.

b. How long does it take to install/deploy Oracle AVDF? Is consulting help needed?

A typical proof of concept can range anywhere from 2 days to 2 weeks, depending on the number of targets and policies. There are three key steps to deployment:

1. Installation of the Audit Vault Server and optionally Database Firewall on server machines of their choice: The whole process using the ISO image is quite simple and can be accomplished quickly in

a few hours. If you are deploying Oracle AVDF from Oracle Cloud Marketplace in an OCI tenancy, the system can be provisioned in just a few minutes.

2. Enabling or creating the appropriate audit or monitoring policies on the target or the Database Firewall: Oracle AVDF can help customers create default policies with a few clicks very quickly, but depending upon the use case, this can take more time.
3. Analyzing the reports and alerts: Oracle AVDF provides several dozen reports out-of-the-box, and you can customize them further to address your compliance or security requirements.

Once the proof of concept is done, you would typically spend more time setting up backup, archival, high availability, etc., using the Oracle AVDF console. You can also use the custom collector framework to add collectors for your applications.

Many of our customers have implemented Oracle AVDF without using consulting services.

Before installation, refer to the installation checklist in the Installation Guide and use the sizing spreadsheet (MOS Note: 2092683.1) to determine the appropriate hardware configuration.

c. How does Oracle AVDF minimize deployment and upgrade time?

Oracle AVDF is a full-stack software appliance that includes the Oracle Linux operating system, Oracle Database, and the Oracle AVDF software, making it easy to deploy and upgrade all components at once. When the Audit Vault Server is upgraded, the agents are automatically downloaded and updated, thus minimizing deployment and upgrade time.

d. What is Oracle's support policy when additional or third-party software is Installed on Oracle AVDF?

Oracle Audit Vault and Database Firewall (AVDF) is shipped as an appliance, and no third-party software should be installed on the Audit Vault Server. See Oracle AVDF Concepts Guide for more details.

6. UPGRADE

a. I currently have Oracle AVDF 12.2. Why should I upgrade to Oracle AVDF 20?

You should consider upgrading to Oracle AVDF 20 for the following reasons:

- Oracle AVDF 12.2 ended premier support in March 2021. That means Oracle is no longer producing periodic security patches for the product.
- Brand new and modernized UI optimized for different workflows, which increases admin/auditor productivity.
- Support for unified audit is important to customers looking to move from traditional to unified audit.
- Simplified configuration of the Database Firewall settings compared to earlier releases.
- New targets such as PostgreSQL, MongoDB (using a simple attribute mapping table), Oracle Cloud autonomous databases
- Extended custom collector support to include JSON, REST, and CSV
- Collection of before/after values of modified records, using Oracle GoldenGate Integrated Extract process (restricted license included) that supports multi-tenant Oracle DB configurations.
- Active Directory integration makes it easier to manage Oracle AVDF users centrally.
- Automated archival of audit/network event data from the Audit Vault Server.
- **FIPS 140-2** compatibility for embedded database and operating system
- Ability to deploy **Oracle AVDF** on-premises or in the **Oracle Cloud**
- Security Technical Implementation Guidelines (STIG) unified audit policy for provisioning on Oracle Database targets.

A list of the significant new features and enhancements introduced in **Oracle AVDF 20** and **later release updates** can be found *here*. If you want to see these features in action, then register for **LiveLabs** guided workshop *here*.

b. What Oracle AVDF versions can I upgrade from?

You can upgrade from Oracle AVDF 12.2.0.9.0 and above to Oracle AVDF 20. If you are on a version lower than 12.2 BP9, you should upgrade it first. See Oracle AVDF Installation Guide for details.

c. Would my currently registered targets, customized reports, and archived data migrate?

After the upgrade, your currently registered targets, customized reports, and archive data will be automatically migrated to Oracle AVDF 20.

7. MORE INFORMATION

a. How do I start using Oracle AVDF? What resources are available?

Visit the Oracle Technology Network website to learn more about the product and access white papers, datasheets, and other materials, or contact an Oracle representative near you.

b. Where can I download the Oracle AVDF software and the product documentation?

Oracle AVDF is available for download from Oracle Software Delivery Cloud. Go to Oracle Software Delivery Cloud and search for the Oracle Audit Vault and Database Firewall product pack.
Oracle AVDF is also deployable on the Oracle Cloud. Navigate to https://cloudmarketplace.oracle.com/ and search for “Oracle Audit Vault and Database Firewall.”

Product documentation is available here.

c. Is there an external discussion forum?

Yes, Oracle Audit Vault and Database Firewall forum provide a platform where you can get answers to your product questions from Oracle community experts.

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