ORACLE

Audit Vault and Database Firewall 20

Frequently Asked Questions

July 2020

PURPOSE

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

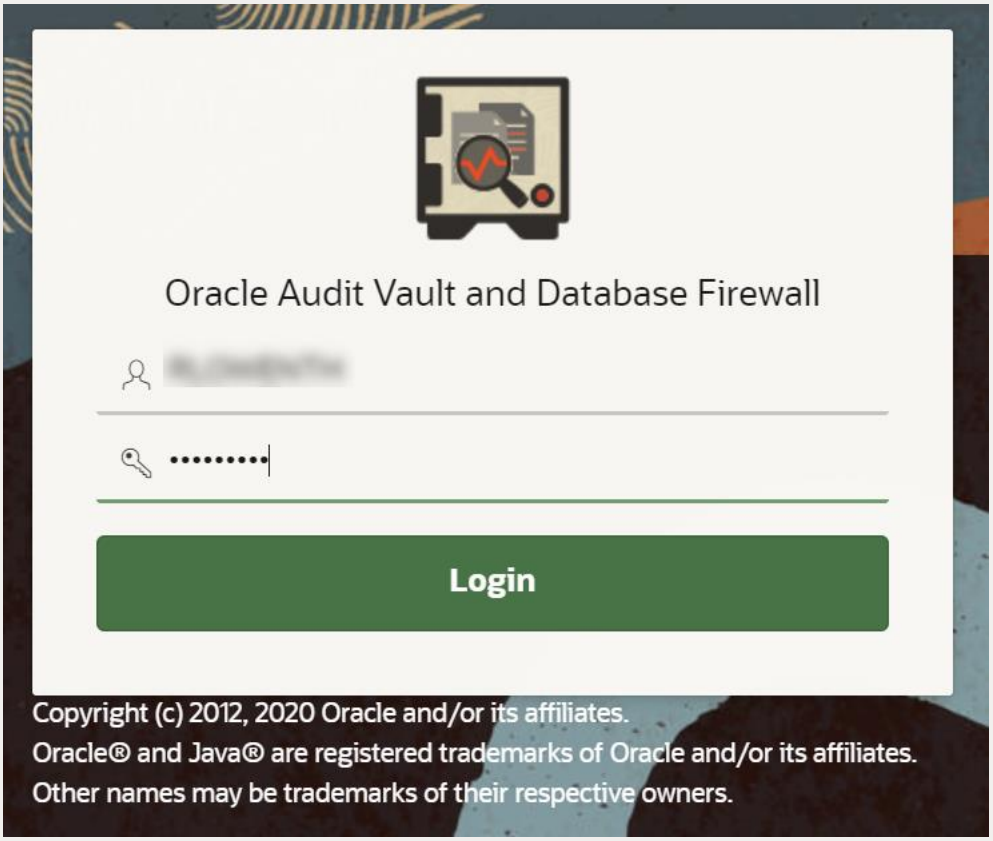
INTENDED AUDIENCE

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 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, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.



1. PRODUCT OVERVIEW

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

AVDF 20 has a revamped and modern user interface with simplified navigation for common workflows, expanded audit collection for new target types (PostgreSQL, MongoDB using a simple attribute mapping table), simplified firewall, and additional features for enterprise support. Refer to the AVDF 20.1 Release Notes for a complete feature list. See the "More information" section below for links to PowerPoints, datasheet, and other resources.

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

AVDF supports native audit collection and network-based SQL traffic monitoring. Audit data is stored in the Audit Vault Server, along with 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 both 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 AVDF?

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

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

AVDF can collect audit data from application tables or files (XML, JSON), map them to the standard format, and include them in a single report across all sources. For details, refer to the 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 has occurred, 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 of these cases, you can specify the conditions under which you want to collect the audit or the event logs. Both of them give different views into the same event, one after, and one before. Alerts can be raised on both of them.

Oracle recommends a holistic approach and supports both 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?

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. 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 both monitoring and blocking or only for monitoring. To implement monitoring and blocking, you need to 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 setup 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, AVDF provides a report that displays details of database events correlated with the original Linux OS user before SU or SUDO transition.

2. KEY USE CASES

a. How does AVDF help meet compliance reporting requirements?

AVDF provides pre-built compliance reports for GDPR, PCI, GLBA, HIPAA, IRS 1075, SOX, and UK DPA. You can customize the reports to meet your specific objectives or your industry/region-specific compliance requirements. Third-party reporting tools can also connect to the Audit Vault schema for analysis and reports.

b. Can AVDF audit and track privileged user's activities?

You can enable audit policies for admin activity and named users. AVDF has pre-defined reports, including privileged user report, which shows all audit activity by privileged users.

c. Can 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). AVDF uses this list to generate pre-defined reports like activity on sensitive data, activity on sensitive data by privileged users, etc.

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

AVDF users can use the "All Activity Report" to analyze which objects were accessed. AVDF can filter by user, object, dates, etc. and analyze the resulting data to see if any unauthorized users accessed the objects.

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

AVDF can be configured to check entitlements on a scheduled basis and provide differential reporting on what has changed since the last report. 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. AVDF captures the before/after values using the Oracle GoldenGate Integrated Extract process (restricted license included) and makes those available in the AVDF reports for analysis. See AVDF Administrators Guide and Auditors Guide for details.

g. How does AVDF help with Database Activity Monitoring (DAM) and SIEM initiatives?

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

AVDF encrypts collected data using Transparent Data Encryption, and it encrypts the network traffic from the targets. 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 AVDF Administrator's Guide for details.

c. Can AVDF use Active Directory for authentication?

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

4. ENTERPRISE CAPABILITIES

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

When configured as 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, 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 AVDF handle the high load from Oracle Exadata, clustered databases, etc.?

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. Refer to the "Audit Vault and Database Firewall Best Practices and Sizing Calculator" (MOS Note: 2092683.1) for sizing guidance.

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

On-premises Audit Vault Server collects audit data from both Oracle Database Cloud Service (DBCS) and on-premises database instances. The on-premises (or on the cloud) Audit Vault agent(s) collect audit data from database instances in DBCS. Currently, Audit Vault Server collects data for traditional audit trail, 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 AVDF support high availability for fault tolerance?

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. Refer to the Administrator's Guide for details.

e. Can 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 to a low-cost external repository and retrieved as per the target-specific policy. Refer to the Administrator's Guide for details.

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

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

g. How is AVDF integrated with Oracle security products such as Database Vault and DBSAT?

The output of the Database Security Assessment Tool (DBSAT) containing the list of sensitive columns/tables in your schema can be imported into AVDF, and audit activity on these tables can be viewed in the AVDF Reports. AVDF can read audit data from the Database Vault audit trail and display it in the AVDF Reports.

5. DEPLOYMENT

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

Any Intel x86 64-bit hardware platform that is supported by Oracle Linux release 7 can be used to deploy the AVDF components. For a complete list of certified hardware, please refer to the Hardware Certification List. Each Audit Vault Server and each Database Firewall must be installed on its own dedicated x86 64-bit server.

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

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

A typical proof of concept can range anywhere between 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 itself is quite simple and can be accomplished quickly in a few hours.
2. Enabling or creating the appropriate audit or monitoring policies on the target or on the Database Firewall: 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: 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, then you would typically spend more time setting up backup, archival, high availability, etc. using the AVDF console. You can then also use the custom collector framework to add collectors for your own applications.

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

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

c. How does AVDF minimize deployment and upgrade time?

AVDF is a full-stack software appliance that includes the Oracle Linux operating system, Oracle Database, and the 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.

6. UPGRADE

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

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

- Brand new and modernized UI that is optimized for different workflows, which increases admin/auditor productivity.
- Support for unified audit, which 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).
- 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 making it easier to centrally manage AVDF users.

- Automated archival of audit/network event data from the Audit Vault Server.
- Note that AVDF support ends on March 2021, and new features will be added mainly to AVDF 20. Hence you should definitely consider upgrading to AVDF 20.

b. What AVDF versions can I upgrade from?

You can upgrade from AVDF 12.2.0.9.0 and above to AVDF 20. If you are on a version lower than 12.2 BP9, you should upgrade to 12.2 BP9 first and then upgrade to AVDF 20. See 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 would be automatically migrated to AVDF 20.

7. MORE INFORMATION

a. How do I start using 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 AVDF software? Product documentation?

AVDF is available for download from Oracle Software Delivery Cloud. Go to Oracle Software Delivery Cloud and search for product pack: 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 provides a platform where you can get answers to your product questions from Oracle community experts