Frequently Asked Questions

Oracle Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall (AVDF) consolidates database activity monitoring events and audit data from databases, operating systems, and directories.

AVDF Deployment

Q: Where can I download the media pack?

A: Oracle Audit Vault and Database Firewall 12.2 is available for download from Oracle Software Delivery Cloud:

Go to https://edelivery.oracle.com;

Select Product Pack: Oracle Database with Platform: Linux x86-64.

Q: What type of hardware platform can I use?

A: Any hardware that supports Oracle Linux for x86-64 Release 6 Update 6 can be used to deploy the Oracle Audit Vault and Database Firewall server components. For a complete list of certified hardware, visit https://linux.oracle.com/hardware.html.

Q: How does the software appliance install work?

A: Oracle Audit Vault and Database Firewall is packaged as a soft-appliance, which means it contains everything needed to install the product on bare hardware, including the operating system. During installation, it completely takes over the hardware. It re-partitions and reformats the disks, installs base OS (Oracle Linux 6.6), user-space libraries, Oracle Database, Oracle Audit Vault and Database Firewall software etc. It configures all the software (OS, networking, Database and so on) almost automatically, with minimal user involvement.

Q: Which network cards can be used with the Database Firewall?

A: All network cards supported out of the box by Oracle Linux 6 release 6 can be used with Audit Vault and Database Firewall. When Database Firewall is deployed in-line, it is sometimes desirable to use a network interface card with bypass to allow continuous SQL traffic flow to the database in the case of a hardware failure.

The following bypass network cards are

Supported from AVDF BP5:

Copper 10/100/1000

- Interface Masters Niagara 32264

Fiber 10/100/1000 (SX and LX) for PCI-x

- Interface Masters Niagara 2282 (Dual)
- Interface Masters Niagara 2283 (Quad).

Fiber 10/100/1000 (SX and LX) for PCI-e

- Interface Masters Niagara 2285 (Dual)
- Interface Masters Niagara 2284 (Quad)

Fiber 10G (PCI-E)

- Interface Masters Niagara 32710 (Dual)

Q: Can I deploy the product on Windows?

A: Oracle Audit Vault and Database Firewall can only be deployed on bare metal and not on a host with a pre-installed operating system such as Windows. The Oracle Audit Vault Agents, however, are deployed on the systems that can run on operating systems including Linux/x86-64, Windows/x86-64, Solaris/SPARC64, Solaris/x86-64, and AIX/POWER64. Please refer to product documentation for the full list of supported platforms.

Q: Can I run using an Oracle Virtual Machine?

A: Although Oracle Audit Vault and Database Firewall can be run on OVM, Oracle does not encourage customers to do so. For testing or proof of concept purposes, it is sufficient to run Oracle Audit Vault and Database Firewall in two Oracle VMs on a single physical server. However, for production deployment, Oracle Audit Vault Server and Database Firewall should be installed on two dedicated physical boxes.

Q: What hardware do I need?

A: Oracle Audit Vault and Database Firewall is comprised of two primary components – the repository or Audit Vault Server and the Database Firewall. The Audit Vault Server functions as the central repository and manager of one or more Database Firewalls. A single Audit Vault Server communicates with and consolidates information from one or more Database Firewalls. The Audit Vault Server also consolidates audit data from the backend databases as well. The Database Firewall is also a dedicated server. A single Database Firewall can monitor hundreds of individual databases depending on its deployment in the network topology.

Q: Can I use an Oracle Database Appliance?

A: No, at this time Oracle Audit Vault and Database Firewall is not certified with the Oracle Database Appliance.

Q: How much storage do I need?

A: 250GB is the minimal required amount of disk space for Audit Vault Server and Database Firewall, but the exact requirements depend on the amount of data being collected and the data retention policy.

Q: How are Agents downloaded and deployed?

A: In Oracle Audit Vault and Database Firewall 12.2 there is one Agent file: agent.jar.The file is the same, regardless of the host, or the platform the host runs on. The agent is linked to the Audit Vault Server repository it was downloaded from. The Agent can only run on a 64-bit OS and it requires a 64-bit JRE. However, it can be used to remotely connect to a database that is running on a 32-bit environment for auditing.

Q: How do I upgrade from the current product?

A: Oracle Audit Vault and Database Firewall 12.1.x installations can be upgraded to the new 12.2 version in-place by simply inserting the 12.2 installation DVD and running the upgrade script. At this time there is no direct upgrade/migration path from legacy releases of Oracle Audit Vault 10.3 or Oracle Database Firewall 5.2 to 12.2. We are planning to provide migration scripts at a future time to assist with moving the data from the existing Oracle Audit Vault repository to the latest 12.2 product.Meanwhile, we encourage customers to continue running their existing Oracle Audit Vault installations and Database Firewall installations for their existing databases.Premier Support for Oracle Database Firewall 5.x and Oracle Audit Vault 10.3 do not end until January and December 2016, respectively. See

http://www.oracle.com/us/support/library/lifetime-support-technology-069183.pdf

Q: Can I migrate my customized reports from 10.3 to 12.2?

A: There are schema changes as we enhanced the new product to support multiple audit source types; therefore, the existing Oracle BI Publisher reports need to be updated.

Q: Is host monitoring supported?

A: Oracle Audit Vault and Database Firewall 12.2 supports host monitoring for Linux, Windows, Solaris SPARC and Solaris x64 platforms. We plan to provide other platform support such as AIX, and HP-UX in the future.

Q: Can I consolidate custom Audit Data from applications?

A: Oracle Audit Vault and Database Firewall ships with several prepackaged collection plug-ins, which are software programs that know how to access and interpret audit data from defined secured target systems of various types. Each collection plug-in is specific to a particular type of trail (directory for a file system, or table name for adatabase) from a particular type of secured target. Oracle encourages our customers and partners to build custom plug-ins that collect and

parse from their specific audit trails. Please refer to the Oracle Audit Vault and Database Firewall Developer's Guide for complete details. http://docs.oracle.com/cd/E37100_01/doc.121/e27779.pdf

Q: What protocol is used to secure transport?

A: From Oracle Audit Vault Server to Database Firewall or Oracle Audit Vault Agents we use HTTPS (port 443) and an additional SSL over TCP/IP (port 1514) communication channel from Database Firewall to Audit Vault Server. Between Oracle Audit Vault Server and Oracle Audit Vault Agent we use Oracle Advanced Security (SSL or Native).

Q: How do I reset expired password for AVADMIN?

A: AVADMIN is a standard database user; you can change the password like you would any other database user. You can use SQL*Plus, EM, or any other database client that can issue an 'ALTER USER' command.

Q: Can I export polices from test to production?

A: No, there is no import/export capability at this time. We plan to address this requirement in a future release.

Q: How do I backup the appliances?

A: From release 12.2 Audit Vault Server backup tool is packaged with the product.Pleaser refer to product documentation for instructions on how to use it.

Q: Are there Oracle University training classes available?

A: Oracle University has created formal classes for the 12.1 version of Oracle Audit Vault and Database Firewall product. Most of this material is relevant for the new 12.2 version too. We are working with Oracle University to update the contents of the course with the additions specific to the new Oracle Audit Vault and Database Firewall release 12.2. If you are interested in taking the class, please call 1.800.529.0165 or contact your local Oracle University sales Representative.

Q: Is there an external discussion forum?

A: Yes. The Oracle Audit Vault and Database Firewall forum can be found on OTN under the Database Security category. Please visit https://forums.oracle.com/forums/forum.jspa?forumID=1420 for discussions andquestions.

Q: What about high availability?

A: You can find HA deployment description in the Oracle Audit Vault and Database Firewall Administrator's Guide.

Q: Where do I go to learn more?

A: Product documentation can be found at http://docs.oracle.com/cd/E37100_01/index.htm Also, visit Oracle Audit Vault and Database Firewall in Oracle Products and Services website for white papers, data sheets, and other materials or contact an Oracle representative near you: http://www.oracle.com/corporate/contact/index.html.

ORACLE

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200