An Oracle White Paper
May 2013

Oracle Audit Vault and Database Firewall 12.1 Sizing Best Practices

Introduction

Oracle Audit Vault and Database Firewall provides a first line of defense for databases and consolidates audit data from databases, operating systems, and directories. A highly accurate SQL grammar-based engine monitors and blocks unauthorized SQL traffic before it reaches the database. Database activity data from the network is combined with detailed audit data for easy compliance reporting and alerting. With Oracle Audit Vault and Database Firewall, auditing and monitoring controls can be easily tailored to suit numerous environments with seamless support for an extensive range of hardware platforms, assuring that a deployed architecture can scale for future growth.

This guide contains four sections. The first section provides a brief overview of the Oracle Audit Vault and Database Firewall components. The second section provides a method for determining hardware requirements for the Database Firewall component. The third section focuses on determining hardware requirements for the Audit Vault Server component. The fourth section outlines the issues that will determine the placement and number of Oracle Database Firewalls and Audit Vault Servers throughout the enterprise.

Component Overview

Oracle Audit Vault and Database Firewall deployments are comprised of three primary components: the Audit Vault Agents, the Database Firewalls, and the Audit Vault Server.

The Audit Vault Server component consolidates monitored database activity and audit data from databases, operating systems and directories into a single unified repository and contains extensive out-of-the-box reporting facilities for compliance and/or incident investigation. In addition to performing warehouse functions for database activity events and audit logs, the Audit Vault Server provides a web interface for centralized configuration and administration of Audit Vault Agents and Database Firewalls. A single Audit Vault Server can aggregate audit data, monitor and configure hundreds of Database Firewalls and Audit Vault Agents simultaneously. Audit Vault Servers can be deployed in a high availability mode for disaster recovery.

Audit Vault Agents are usually installed directly onto the host operating system of the Secured Target (the database, operating system, or file system being monitored). They manage collection of all audit information from the targets' native audit trails via built-in or custom Collection Plugins. In some cases Audit Vault Agents can be installed on other hosts and access audit trails remotely over the network. In production deployments there is usually a one-to-one ratio between Agents and Secured Targets, and one-to-many between Agents and Collection Plugins they operate. The collected audit event data is propagated onto the Audit Vault Server the Agent has been paired with at installation time. Oracle Audit Vault and Database Firewall comes with built-in support for collection of audit information from Oracle, IBM DB2 LUW, Microsoft SQL Server, SAP Sybase ASE and MySQL databases as well as Oracle Solaris, Linux, Microsoft Windows operating systems, Microsoft Active Directory services and Oracle ACFS file system.

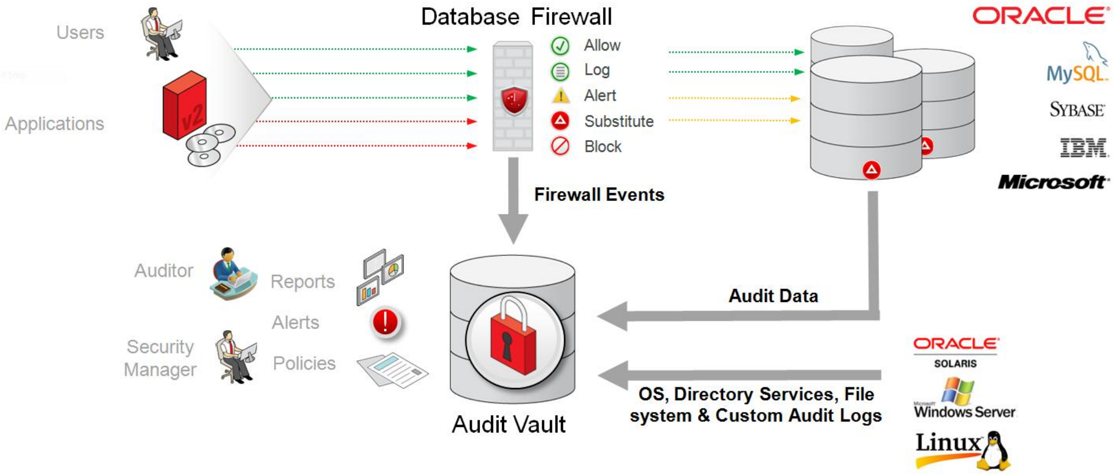

Figure 1. Audit Vault and Database Firewall Architecture

Database Firewalls are components in the Audit Vault and Database Firewall deployment that are placed in-line or out-of-band on the network to inspect network traffic. The Database Firewall operates in two modes depending on your security and operational needs:

- Database Activity Monitoring (DAM): The system detects and logs unusual activity, and produces warnings, but does not block potential threats. This is also known as monitoring mode.
- Database Policy Enforcement (DPE): The system performs all the actions of database activity monitoring and blocks potential attacks. This is also known as blocking mode.

A single Database Firewall can provide heterogeneous, simultaneous multi-database policy enforcement for Oracle, MySQL, Microsoft SQL Server, SAP Sybase ASE, SAP Sybase SQL Anywhere, and IBM DB2 LUW databases.

Sizing Hardware Requirements

Audit Vault Server Sizing

The primary factors in planning Audit Vault Server capability is the cumulative number of transactions per second logged onto the server and the length of the retention policy for stored audit information. Audit records from all attached Database Firewalls and Audit Vault Agents need to be included when considering Audit Vault Server sizing.

Disk

The minimal required HDD size to install and run Audit Vault Server is 150GB. However for most real-world installations disk space should be considerably larger. The two most important factors that determine HDD requirements are per-second rate of recording audit events and the length of the retention period as specified by the active retention policy for each Secured Target.

The size of the audit event warehouse can be estimated by aggregating storage space requirements for event data from all protected Secured Targets. As individual Secured Targets can be monitored using Database Firewalls and/or audited via Audit Vault Agent, the calculation should include estimated audit event rates for all Audit Trails and Enforcement Points configured for the Secured Target. Logging event rate for a Secured Target from the Database Firewall should be adjusted by the SQL complexity factor (see detailed explanation in the corresponding section below). Average size of the audit record should be taken as equal to the average size of the audited SQL statement or, if unknown, can be assumed to be 512 bytes (approximately 0.00000048 GB). On the basis of these rates a daily volume of audit information stored for a Secured Target can be calculated as follows:

$$V_D = (A_D + (F_D \times C)) \times S$$

Where:

V_D Daily volume of audit data for the a Secured Target (in GB)

A_D Per-day audit record insertion rate from Audit Vault Agent deployed for a Secured Target

F_D Per-day event record insertion rate from Database Firewall protecting a Secured Target

C Database Firewall Statement Complexity Factor (see below)

S Average size of audit record (in GB)

To calculate the storage requirement for audit information for a Secured Target, the daily volume of audit data needs to be multiplied by the length of the retention period (in days) as shown:

$$V = V_D \times L$$

Where:

V Storage requirement for audit event data for a Secured Target (in GB)

V_D Daily volume of audit data for the a Secured Target (in GB)

L Length of the retention period for a Secured Target (in days)

The size of the event warehouse storing all audit event data can be calculated by aggregating storage requirements across all Secured Targets:

$$W = \sum V$$

Where the sum $\sum$ is performed across all Secured Targets and:

W Estimated size of the audit event warehouse (in GB)

V Storage requirement for audit event data for each Secured Target (in GB)

The overhead of storing and managing audit information in the internal repository on Audit Vault Server is usually under 10% of the volume of the stored audit information. Other functions of the Audit Vault Server require an additional 50GB of storage space regardless of the volume of audit data. Thus the basic rule for estimating disk space (in GB) for Audit Vault Servers can be represented as the following formula:

$$D = W + (W \times 0.1) + 50$$

Where:

D Required HDD size (in GB)

W Estimated size of the audit event warehouse (in GB)

Database Firewall SQL Complexity Factor

SQL events produced by Database Firewalls contain the exact SQL statement as captured from the network during client-database interactions. When these events are stored in the Audit Vault repository each of these statements may result in multiple event records inserted into the event warehouse. This depends on the complexity of the statements in terms of the number of 'target' objects – usually tables – featured in the SQL. For each 'target object' in the original SQL there would be a separate audit record stored in the event repository. The complexity factor featured in the formulas in this paper as C is the number of target objects (tables) addressed in an 'average' SQL statement logged by Database Firewall.

CPU

Audit Vault Server CPU capacity is utilized by the following two main functions: recording audit events delivered by Audit Vault Agents, and processing and storing SQL traffic records from Database Firewalls. There are two less CPU-intensive auxiliary functions: producing reports and generating alerts. The number of CPU cores required for processing audit records from Audit Vault Agents can be estimated by allocating one core for every 1,000 audit records per second (RPS) stored onto Audit Vault Server. This assumes the average size of an audit record to be around 512 bytes. A similar logic should be applied to traffic events captured by Database Firewall, however, in this case the complexity of the logged statements needs to be taken into account (see corresponding section above). The formula can be expressed as follows:

$$N = \frac{A_{\Sigma}}{1000} + \frac{(F_{\Sigma} \times C)}{1000} + 1$$

Where:

N Number of CPU cores required

A_{Σ} Cumulative audit record insertion rate from all Audit Vault Agents (in records per second)

F_{Σ} Cumulative event record insertion rate from all Database Firewalls (in records per second)

C Database Firewall statement complexity factor (see above)

1 One CPU core dedicated to basic system management functions

The A_{Σ} and F_{Σ} cumulative rates represent the aggregate recorded per-second audit event rates across all Audit Trails and Enforcement Points respectively for all Secured Targets of the Audit Vault Server.

Further CPU considerations

A further recommendation can be made for deployments with many low-throughput databases and other audited data assets. The ratio between the number of Secured Targets to the number of cores in the system should not exceed 10, in other words the following condition should be met:

$$\frac{T}{N} \leq 10$$

Where:

T Number of Secured Targets to be configured in the Audit Vault Server

N Estimated number of cores for the Audit Vault Server

Memory

The minimal required RAM to install and run the Audit Vault Server is 2GB. In addition to this, RAM space should be provisioned for each Secured Target which is to be managed by the Audit Vault Server as shown in Table 1 below.

TABLE 1. ESTIMATED RAM REQUIREMENTS FOR DIFFERENT USAGE PROFILES

USEAGE	RAM REQUIREMENTS
Moderate	0.1 GB per Secured Target
Medium	0.25 GB per Secured Target
High	0.5 GB per Secured Target

Database Firewall Sizing

The most important factor in planning for Database Firewall capacity is the cumulative number of transactions per second that the Database Firewall will monitor. The number is derived by aggregating average database transaction rates across all databases that would be monitored by the database firewall.

CPU

The number of CPU cores required can be estimated by allocating one core for every 5,000 transactions per second (TPS) monitored by Database Firewall, plus one core for all system management processes. Table 2 lists the recommended number of CPU cores based on the total rate of SQL transactions per second for all databases protected by Database Firewall.

TABLE 2. ESTIMATED CPU REQUIREMENTS FOR DIFFERENT TRANSACTION PER SECOND (TPS) RATES

CORES	TPS FOR MIXED ENVIRONMENTS	TPS FOR ORACLE	TPS FOR ORACLE WITH ASO	TPS FOR OTHER RDBMS
2	5,600	4,200	3,360	8,400
4	16,800	12,600	10,080	25,200
6	28,000	21,000	16,800	42,000
8	39,200	29,400	23,520	58,800
10	50,400	37,800	30,240	75,600
12	61,600	46,200	36,960	92,400
14	72,800	54,600	43,680	109,200
16	84,000	63,000	50,400	126,000
32	173,600	130,200	104,160	260,400
48	263,200	197,400	157,920	394,800

The “Oracle” column in the table represents the estimated transactions per second that can be read by the Database Firewall. The “Oracle with ASO” column represents the estimated ASO-encrypted TPS that can be processed by the Database Firewall. Depending on the traffic profile, ASO encryption of the traffic has impact in the range of 5% to 20% on the performance of the Database Firewall versus equivalent traffic without encryption enabled. For sizing, it is recommended to use a conservative value close at the upper end of this range. The “Other RDBMS” column in the table represents the number of TPS that can be read by the Database Firewall for the other supported databases. If you have a Database Firewall that is monitoring a combination of heterogeneous RDBMSs, then you can use an estimate of 5,000 TPS, otherwise the numbers in the columns can guide you on the number of CPU cores that are recommended.

Memory

The minimal required RAM to install and run the Database Firewall component is 2GB. For systems with multiple Enforcement Points use the following table to calculate the total required RAM size.

TABLE 3. ESTIMATED RAM REQUIREMENTS FOR DIFFERENT USAGE PROFILES

USEAGE	RAM REQUIREMENTS
Moderate	0.5 GB per Enforcement Point
Medium	1.0 GB per Enforcement Point
High	1.5 GB per Enforcement Point

The system will function with less memory, however, the larger memory sizes are recommended to provide optimal performance during of periods of high throughput.

Disk

The minimal required HDD size to install and run Database Firewall at moderate use is 130GB. The disk is used for temporary storage of captured SQL traffic and associated data before it is transferred to the Audit Vault Server. The disk space should be large enough to retain several days of monitored data in case the communication between Database Firewall and Audit Vault Server is interrupted (e.g, a link failure between data centers).

TABLE 4. ESTIMATED HDD SIZE REQUIREMENTS FOR DIFFERENT USAGE PROFILES

USEAGE	HDD REQUIREMENTS
Moderate	130 GB
Medium	300 GB
High	500 GB

Deployment Planning

Audit Vault Server

Audit Vault Servers represent the top tier in the architecture of Audit Vault and Database Firewall deployments, and as such, should be the first component installed in customer environment. The many-to-one relationship between Database Firewalls, Audit Vault Agents and Audit Vault Server necessarily requires Audit Vault Server capacity to be determined early in the roll-out process. Some large scale deployments could require provisioning of several Audit Vault Servers due to extremely high volumes of audit event data and/or long retention periods. If required, third-party reporting solutions can be used to further aggregate audit event data from multiple Audit Vault Server repositories.

As with Database Firewall policies, the native audit configuration of the Secured Targets needs to be selective to be effective. Audit Vault Agents guarantee that all audit records from the original audit trail are propagated to the Audit Vault Server repository. Sizing estimates produced by the formulas from this paper are only as accurate as the input data used. Care should be taken when assessing the logging/auditing rate, as well as the usage profiles in terms of reporting and other user activity.

Database Firewall Considerations

Given the flexibility of the Database Firewall, deployment planning should start with understanding the existing network infrastructure in the context of security and compliance requirements. Objectives to be considered are:

- Monitoring versus policy enforcement
- Network infrastructure
- Existing resilience and high-availability configuration in the customer environment

SQL Logging Policies

As described in the sizing section of this paper one of the primary factors determining the capacity of the Audit Vault Server will be the logging policy applied to the traffic on Database Firewalls managed by this server. In high through-put environments, a log-all policy is not recommended for the following reasons. Firstly, the amount of data stored (one record for every query sent to the database) will quickly create a repository much larger than the databases being protected. Secondly, a large amount of data often makes forensic and audit reporting more difficult by obscuring important transactions through the sheer volume of data.

Oracle Database Firewall is capable of identifying database queries of significance from a security and/or audit perspective in real time in a sub-millisecond timeframe. The accuracy and speed with which the Database Firewall operates allows the end-user to deploy a selective logging policy, knowing that activity identified as legitimate can be discarded with confidence as a valid part of an accurate white list. Likewise, the end user can also be confident that only interactions relevant to security and audit requirements will be logged and/or alerted. It is important to remember that the vast majority of entries in aDatabase Firewall white list will consist of expected transactions. Audit and security events are identified through a combination of session factors, significant white list entries, polices based on statement-types and sensitive tables, and general out-of-policy events (anomalies).

Network Infrastructure

The number and choice of databases secured by a given Database Firewall depends on the distribution of databases across the network infrastructure. The choice will also be affected by any preference for a particular size of hardware on which to deploy the Database Firewall. For example, depending on current hardware and maintenance costs, it may be more cost-effective to deploy two or three mid-range hosts versus one high performance machine.

The following factors should be considered:

- Distribution Layer - The Distribution Layer of the network is comprised of the group of switches directly attached to database servers. At this level, multiple small-to-mid-sized Database Firewalls are deployed for in-line or span-port monitoring of traffic near the database. If preferred, a smaller number of larger Database Firewalls with multiple network interfaces can be used instead.
- Core Layer - The Core Layer (or network backbone) includes high-end switches and high-speed cables. A small number of larger Database Firewalls can monitor uplink traffic at the core (up to 10GB per network segment) in-line or via span-ports to capture SQL traffic from other segments of the corporate network or from external sources. Note that when Database Firewall is deployed in Database Policy Enforcement (DPE) mode, the databases protected in a given network segment must be in the same subnet as the IP address assigned to the corresponding bridge on the Database Firewall. This restriction does not apply to Database Activity Monitoring (DAM) mode, whether deployed in-line or via a span port.
- Multiple Data Centers - For centralized management, one Audit Vault Server can control Database Firewalls deployed across multiple data centers.
- Distributed Management – Database Firewalls can be managed by a local Audit Vault Server to suit local network topologies. Corporate security and auditing policies may encourage a separation of management between data centers or between departments. Deploying a separate Audit Vault Server may also be desirable where interconnectivity between data centers is limited by bandwidth restrictions or data protection policies.

Resiliency, High-Availability, and Testing

- High Availability Network Environments – Database Firewalls are compatible with a number of resilient network technologies, monitoring both primary and secondary network links. For blocking mode, HA deployments must preserve session integrity across any given Database Firewall bridge, and must utilize standard TCP/IP. When failing over, the HA configuration must also initiate new sessions across the alternate link. In addition, there is a special mode for span-port deployments that allows a resilient pair of Database Firewalls to monitor the same traffic without creating duplicate events.

- Load Balanced Environments – Database Firewalls can be deployed as multiple individual units immediately in front of the database servers to match the performance and high-availability architecture of the secured systems. Load balancers must retain session integrity through any given Database Firewall bridge and must utilize standard TCP/IP.
- Failover/Backup Data Centers – Redundant Database Firewalls can be deployed in backup data centers, running in active mode with the latest policy settings to ensure protection for the backup systems the instant a failover occurs.
- Testing and Development - Most customers find it beneficial to deploy one or more Database Firewalls in their testing and development environments. In addition to the valuable summary of SQL traffic it provides, it can be used to develop and update white list policies before new systems or functionality is released.

Conclusion

The architecture of environments in which Oracle Audit Vault and Database Firewall can be deployed can differ significantly between customers. This paper provides a means of estimating the required hardware capability in terms of memory, disk and processor cores, based on the assessment of existing traffic rates and future logging policies. It uses a simple ‘moderate-medium-high’ approach where possible, and formulas in which detailed consideration of the influencing factors is required.

Oracle is committed to developing practices and products that help protect the environment

Oracle Audit Vault and Database Firewall 12.1
Sizing Best Practices
May 2013
Author: Andrey Brozhko

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Hardware and Software, Engineered to Work Together