

ORACLE AUDIT VAULT

KEY BENEFITS AND FEATURES

- Consolidate and secure audit data from Oracle and Microsoft SQL Server, Sybase and IBM DB2 databases
- Built-in and customizable reports for compliance and monitoring
- Raise alerts on suspicious activity
- Capture before/after values from transaction logs
- Automated cleanup of Oracle database audit data on source systems
- Manage audit policies across Oracle databases
- Scale with robust Oracle Database technology

Satisfying compliance regulations and mitigating security risks are two of the top security challenges businesses face today. Oracle Audit Vault reduces the cost and complexity of compliance and helps detect suspicious activity by automating the collection and consolidation of audit data. It provides a secure and highly scalable audit warehouse, enabling centralized reporting, analysis, and threat detection on audit data.

Monitoring for Security, Compliance, and Privacy

Sarbanes-Oxley (SOX), Payment Card Industry (PCI), and regional privacy directives are just a few of the regulations and industry standards that require a multi-faceted approach to security. Businesses not only have to protect sensitive information, but also monitor access to sensitive information for both compliance and potential threats.

Examination of numerous data breaches has shown that auditing could have helped detect problems early, reducing the financial impact. Oracle Audit Vault transparently collects and consolidates audit data, providing valuable insight into *who did what* to *which* data *when* – including privileged users who have direct access to the database.

With Oracle Audit Vault reports, alert notifications, and centralized audit policy management, the risks from internal threat and the cost of compliance are greatly reduced. Oracle Audit Vault leverages Oracle's industry leading database security and data warehousing technology for managing, analyzing, storing, and archiving large volumes of audit data. Oracle Audit Vault collects database audit data from Oracle, SQL Server, IBM DB2, and Sybase ASE databases. Oracle Audit Vault supports Oracle9i and higher databases as well as SQL Server 2000 and 2005 releases, Sybase ASE 12.5 through 15.0, and IBM DB2 8.2 and 9.5.

Simplified Compliance Reporting

Oracle Audit Vault provides standard audit assessment reports covering privileged users, account management, roles and privileges, object management and system management across the enterprise. Parameter driven reports can be defined showing user login activity across multiple systems and within specific time periods, such as weekends. Oracle Audit Vault provides an open audit warehouse schema that can be accessed from Oracle BI Publisher, Oracle Application Express, or 3rd party reporting tools



Figure 1. Oracle Audit Vault Overview

RELATED PRODUCTS

- Oracle Database Vault
- Oracle Advanced Security
- Oracle Label Security
- Oracle Secure Backup
- Oracle Data Masking

Object	Event	User	Source	Host	Event Time	SQL Text
OE.CUSTOMER_PAYMENT	SELECT	DE	PAYROLL.Oracle.VM	oekup04.oracle.vm	05-FEB-08 09:48:24	select payment_card_num customer_payment
OE.CUSTOMER_PAYMENT	SELECT	VSHAH	PAYROLL.Oracle.VM	oekup04.oracle.vm	05-FEB-08 09:48:24	select payment_code_id fr customer_payment
OE.CUSTOMER_PAYMENT	SELECT	VSHAH	PAYROLL.Oracle.VM	oekup04.oracle.vm	05-FEB-08 09:48:24	select payment_card_num customer_payment
OE.CUSTOMER_PAYMENT	SELECT	VSHAH	PAYROLL.Oracle.VM	oekup04.oracle.vm	05-FEB-08 09:48:24	select payment_expiration customer_payment
OE.ORDERS	UPDATE	VSHAH	PAYROLL.Oracle.VM	oekup04.oracle.vm	05-FEB-08 09:48:10	
OE.ORDERS	SELECT	VSHAH	PAYROLL.Oracle.VM	oekup04.oracle.vm	05-FEB-08 09:48:10	select order_total from oe.o

Proactive Threat Detection with Alerting

Oracle Audit Vault event alerts help mitigate risk and protect from the insider threats by providing proactive notification of suspicious activity across the enterprise. Oracle Audit Vault continuously monitors the inbound audit data, evaluating audit data against alert conditions. Alerts can be associated with any auditable database event including system events such as changes to application tables, role grants, and privileged user creation on sensitive systems.

Security and Scalability

Protecting audit data is critical to the security and internal controls processes. Oracle Audit Vault protects Oracle, SQL Server, IBM DB2, and Sybase ASE audit data by using Oracle's strong data security technology. Access to the audit data within Oracle Audit Vault is strictly controlled using pre-defined administrative roles. Oracle Audit Vault leverages Oracle's proven data warehousing and partitioning capabilities to achieve massive scalability, a key requirement for any auditing solution. Once consolidated, Oracle Audit Vault will automatically remove Oracle Database audit data on source systems, helping further simplify audit data management. Oracle Audit Vault can optionally be deployed with Oracle Real Application Clusters (RAC), providing high availability and flexibility. Oracle Audit Vault provides the ability to provision and review audit settings in multiple Oracle databases from a central console, reducing the cost and complexity of managing audit settings across the enterprise.

Summary

Oracle Audit Vault provides a secure and scalable solution for consolidating audit data generated by Oracle, Microsoft SQL Server, IBM DB2 and Sybase ASE. Built-in reporting and alerting help enterprises more easily comply with both regulatory and internal reporting requirements. Oracle Audit Vault automates the audit consolidation process, turning audit data into an important security and compliance resource.

Contact Us

For more information about Oracle Audit Vault, please visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.



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

Copyright © 2009, Oracle and/or its affiliates. All rights reserved.

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.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. 0109