

ORACLE AUDIT VAULT

KEY BENEFITS & FEATURES

Oracle Audit Vault

- Simplify Compliance Reporting with Built-in Reports
- Detect Threats Early with Alerts
- Transparently Collect and Consolidate Audit Data
- Protect Audit Data with Oracle Database Vault and Oracle Advanced Security
- Manage Audit Policies across Oracle Databases
- Scale with Robust Oracle Database Technology
- Build Custom Reports against an Open Warehouse Schema

Satisfying compliance regulations and mitigating the risks associated with the insider threat are two of the top security challenges businesses face today. Oracle Audit Vault reduces the cost and complexity of compliance and the risk of insider threats by automating the collection and consolidation of audit data. It provides a secure and highly scalable audit warehouse, enabling simplified reporting, analysis, and threat detection on audit data. In addition, database audit settings are centrally managed and monitored from within Audit Vault, reducing IT security cost.

Compliance, Privacy and Insider Threats

Sarbanes-Oxley (SOX), Payment Card Industry (PCI), Basel II, and various regional privacy directives are just a few of the regulations and industry standards organizations face in today's global business environment. Businesses not only have to protect sensitive information, but also monitor access to sensitive information for compliance and potential threats. Examination of numerous insider crimes has shown that had there been an effective auditing system in place, the resulting financial impact would have been substantially reduced. However, leveraging audit data has proven to be a difficult task due to the fact that audit data is distributed, making analysis, reporting, and alerting difficult.

Oracle Audit Vault

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.

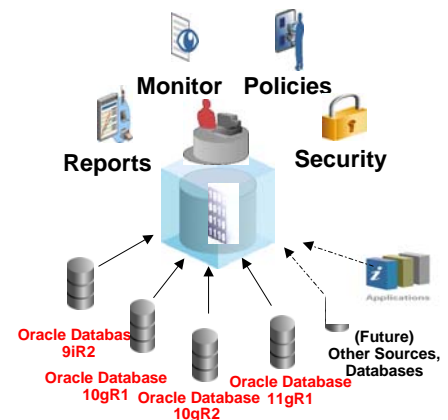


Figure 1. Oracle Audit Vault Overview

Transparent Audit Data Collection and Consolidation

Oracle Audit Vault collects database audit data from the Oracle database audit trails in the database, and on the operating system. Additionally, it can also read the transaction logs to capture the before/after values associated with transactions. Oracle Audit Vault supports Oracle9i Database Release 2, Oracle Database 10g Release 1, Oracle Database 10g Release 2 and Oracle Database 11g Release 1. Future releases will include the ability to collect audit data from non-Oracle databases sources and build custom audit collectors for other sources.

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 any 3rd party reporting tools.

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. Oracle Audit Vault provides graphical summaries of activities causing alerts.

Security and Scalability

Protecting audit data is critical to the security and internal controls processes. Oracle Audit Vault protects audit data by using sophisticated controls including Oracle Database Vault and Oracle Advanced Security. Access to the audit data within Oracle Audit Vault is strictly controlled. Privileged DBA users cannot view or modify the audit data and even auditors are prevented from modifying the audit data. Oracle Audit Vault leverages Oracle's proven data warehousing and partitioning capabilities to achieve massive scalability, a key requirement for any auditing solution. Oracle Audit Vault can optionally be deployed with Oracle Real Application Clusters (RAC), enabling scalability, high availability, and flexibility.

Lowers IT Costs with Oracle Audit Vault Policies

IT security personnel work with auditors to define audit settings on databases and other systems across the enterprise to meet both compliance requirements and internal security policies. Oracle Audit Vault provides the ability to provision and review audit settings in multiple databases from a central console, reducing the cost and complexity of managing audit settings across the enterprise.

Summary

Addressing regulatory compliance requirements and protecting against insider threats in a global economy requires a defense-in-depth approach to security. Oracle Audit Vault automates the consolidation and analysis process, turning audit data into a key security resource to help address today's security and compliance challenges.

Copyright 2007, Oracle. 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 is it 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.