

ORACLE AUDIT VAULT

주요 혜택 및 기능

Oracle Audit Vault

- 내장된 리포트를 이용한 컴플라이언스 리포팅 업무의 단순화
- 경고를 이용한 보안 위협의 탐지
- 감사 데이터의 투명한 수집 및 통합
- Oracle Database Vault, Oracle Advanced Security를 이용한 감사 데이터의 보호
- 전체 오라클 데이터베이스 환경의 감사 정책 관리
- 오라클 데이터베이스 테크놀로지의 강력한 확장성
- Open Warehouse Schema 기반의 맞춤형 리포트 지원

오늘날의 기업들이 당면한 가장 중요한 보안 이슈로 관련 법규의 준수, 그리고 내부자 위협에 관련한 리스크 경감 문제를 꼽을 수 있습니다. Oracle Audit Vault는 감사 데이터의 수집 및 통합 과정을 자동화함으로써 컴플라이언스, 내부자 위협에 관련된 비용과 복잡성을 경감해 줍니다. 뛰어난 보안 수준과 확장성을 지원하는 감사 데이터 웨어하우스 환경이 제공되므로 감사 정보를 이용한 리포팅, 분석, 위협 탐지 업무를 단순화할 수 있습니다. 또 데이터베이스 감사 정책을 중앙 집중적으로 관리, 모니터링하고 IT 보안 비용을 절감하는 것이 가능합니다.

컴플라이언스, 개인정보보호, 내부자 위협

사베인즈-옥슬리(SOX), PCI(Payment Card Industry), 바젤 II 등은 오늘날 글로벌 비즈니스 환경이 당면한 법규/정책 준수 문제의 극히 일부 사례에 불과합니다. 기업은 고객의 기밀 정보를 보호하는 한편으로 컴플라이언스 요건 준수 또는 보안 위협의 차단을 위해 기밀 정보에 대한 접근을 모니터링해야 합니다. 그간 기업 환경에서 발생한 내부자 범죄 사례들의 분석 결과, 효율적인 감사 시스템이 마련되어 있었다면 사고로 인한 금전적 피해를 극적으로 줄일 수 있었을 것이라는 결론이 제시되었습니다. 하지만 감사 데이터를 활용하기란 그리 쉽지만은 않습니다. 감사 데이터는 대부분 여러 위치에 분산된 상태로 관리되고 있기 때문입니다.

Oracle Audit Vault

Oracle Audit Vault는 감사 데이터를 투명한 방식으로 수집, 통합함으로써 (수퍼 유저를 포함하는) 전체 사용자들이 언제, 어떤 데이터에 어떤 작업을 수행했는지 파악할 수 있게 합니다. Oracle Audit Vault의 리포트, 경고 기능과 중앙 집중적 감사 정책 관리 환경을 이용하여 내부자 위협의 리스크와 컴플라이언스 비용을 극적으로 절감할 수 있습니다. Oracle Audit Vault은 오라클의 업계 선두 데이터베이스 보안, 데이터 웨어하우스 테크놀로지를 기반으로 대량의 감사 데이터를 효율적으로 관리, 분석, 저장, 아카이브 합니다.



그림 1. Oracle Audit Vault 개요

감사 데이터의 투명한 수집 및 통합

Oracle Audit Vault는 데이터베이스와 운영 체제에 저장된 데이터베이스 감사 데이터를 수집합니다. 또 트랜잭션 로그에 대한 읽기 작업을 통해 트랜잭션 이전/이후의 값을 캡처하는 기능 또한 지원됩니다. Oracle Audit Vault는 Oracle9i Database Release 2, Oracle Database 10g Release 1, Oracle Database 10g Release 2와 Oracle Database 11g Release 1을 지원합니다. 향후 버전에서는 써드 파티 데이터베이스 소스로부터 감사 데이터를 수집하는 기능과 사용자 정의 감사 데이터 수집기(Collector)가 추가로 구현될 예정입니다.

컴플라이언스 리포팅 업무의 단순화

Oracle Audit Vault는 전사적인 계정 관리, 역할/권한/오브젝트 관리, 시스템 관리를 위한 표준 감사 리포트를 제공합니다. 매개변수 기반 리포트를 통해 여러 시스템에, 또는 일정 시간대에 걸친 사용자의 로그인 활동을 추적할 수 있습니다. Oracle Audit Vault의 감사 데이터 웨어하우스는 개방형 스키마를 지원하므로 Oracle BI Publisher, Oracle Application Express 또는 다른 써드 파티 리포팅 툴을 통해 접근 가능합니다.

경고를 이용한 보안 위협의 사전예방적 탐지

Oracle Audit Vault의 이벤트 경고 기능을 이용하여 의심스러운 활동을 사전예방적으로 탐지함으로써 내부자 위협으로 인한 리스크를 경감할 수 있습니다. Oracle Audit Vault는 수집되는 감사 데이터를 지속적으로 모니터링하면서 사전 정의된 경고 조건에 부합되는지 평가합니다. 애플리케이션 테이블의 변경, 역할 변경, 슈퍼 유저 계정의 생성 등 감사 내역에 포함된 모든 시스템/데이터베이스 이벤트를 기준으로 경고를 설정할 수 있습니다. Oracle Audit Vault는 발생한 경고에 관련된 활동에 대한 그래픽 요약 화면을 제공합니다.

보안과 확장성

감사 데이터를 보호하는 것은 보안 및 내부 컨트롤 프로세스에서 매우 중요한 비중을 차지합니다. Oracle Audit Vault는 Oracle Database Vault, Oracle Advanced Security 등을 포함하는 정교한 컨트롤 기능을 통해 감사 데이터를 보호합니다. Oracle Audit Vault 내부의 감사 데이터에 대한 접근은 엄격하게 통제됩니다. DBA 권한을 가진 사용자도 감사 데이터를 조회하거나 변경할 수 없습니다. 심지어 감사 담당자라 하더라도 감사 데이터를 함부로 변경하는 것이 불가능합니다. Oracle Audit Vault는 오라클의 검증된 데이터 웨어하우징, 파티셔닝 테크놀로지를 기반으로 극대화된 확장성을 제공합니다. 또 Oracle Audit Vault의 확장성, 가용성, 유연성을 개선하기 위해 Oracle Real Application Clusters (RAC) 환경에 구축할 수도 있습니다.

Oracle Audit Vault 정책을 이용한 IT 비용의 절감

IT 보안 담당자들은 컴플라이언스 요건과 내부 보안 정책의 준수를 위해, 감사 업무 담당자들과 함께 데이터베이스 및 기타 시스템의 감사 정책을 설정합니다. Oracle Audit Vault의 중앙 집중적 관리 콘솔을 이용하여 다수 데이터베이스의 감사 설정을 확인, 변경하고 전사적인 감사 정책 관리의 관리에 수반되는 비용과 복잡성을 절감할 수 있습니다.

요약

기업이 컴플라이언스 요건을 준수하고 내부자 위협을 효과적으로 차단하기 위해서는 보다 심층적인 보안 전략이 필요합니다. Oracle Audit Vault는 감사 데이터의 통합/분석 프로세스를 자동화하고 감사 데이터를 핵심 보안 리소스로 활용함으로써 오늘날 기업의 보안, 컴플라이언스 문제를 해결할 수 있도록 지원합니다.

Copyright 2007, Oracle. All Rights Reserved.

본 문서는 정보 제공만을 목적으로 제공되며, 문서의 내용은 사전 공지 없이 변경될 수 있습니다. 본 문서에는 오류가 포함되어 있을 수 있으며, 상업성 또는 특정 목적의 부합성에 대한 명시적, 묵시적인 일체의 보장을 제시하지 않고 있습니다. 오라클은 본 문서에 관련하여 직접적/간접적으로 발생하는 일체의 법적 책임 또는 계약상의 의무를 거부합니다. 본 문서는 오라클의 사전 서면 승인 없이 어떤 목적, 어떤 방법으로도 전자적/기계적인 형태로 복제, 전송될 수 없습니다.

오라클은 Oracle Corporation 및 계열사의 공식등록상표입니다. 다른 이름은 해당 업체의 공식등록상표일 수 있습니다. June 2007