

ORACLE LABEL SECURITY



주요 기능 및 혜택



- 민감도 레이블 (sensitivity label)을 사용한 투명한 로우 레벨 액세스 컨트롤
- Oracle Database Vault와의 통합
- 정책 기반 관리 모델을 통해 동일 데이터베이스에서 여러 가지 정책을 적용 가능
- 가상 컬럼을 이용하여 기존 애플리케이션 SQL에 대한 완전한 투명성 제공
- 정부/방위 기관을 위한 멀티-레벨 보안 지원
- EAL4+ Common Criteria 인증 획득
- Oracle Database 11g Enterprise Edition Security Option – Oracle8i Enterprise Edition Database 이후 버전에서 지원

Oracle Label Security는 민감도 레이블 (sensitivity label)을 이용하여 오라클 데이터베이스의 투명한 로우 레벨 액세스 컨트롤을 구현하는 솔루션입니다. Oracle Database Vault과 함께 적용하는 경우, 민감도 레이블은 컴플라이언스 요구 사항의 해결을 위한 멀티-팩터 권한 할당 (multi-factor authorization)에서 매우 유용하게 활용될 수 있습니다. Oracle Label Security는 매우 유연하고 적응성 있는, 업계 선두의 레이블 기반 액세스 컨트롤 제품입니다. 정책 기반 관리를 통해 민감도 레이블 및 사용자 레이블 권한 관리 업무를 단순화할 수 있습니다.

기밀 데이터의 보호

Oracle Label Security는 데이터 민감도 수준 (data sensitivity level)과 사용자 레이블 권한 (user label authorization)을 비교함으로써 애플리케이션 데이터에 대한 액세스를 투명하게 컨트롤합니다. 보안 관리자는 Oracle Enterprise Manager를 이용하여 데이터 민감도 레이블을 정의하고 사용자에게 접근 가능한 최대 민감도 레이블을 포함하는 레이블 권한을 할당합니다. 보안 관리자는 하나 또는 그 이상의 레이블에 Label Security 정책을 적용할 수 있습니다. Oracle Label Security는 사용자 레이블 권한과 데이터에 할당된 민감도 레이블을 비교함으로써 애플리케이션 데이터에 대한 액세스를 투명하게 중재합니다. 사용자 레이블 권한이 데이터 민감도 레이블과 같거나 큰 경우에만 데이터에 대한 접근이 허용됩니다. 데이터베이스 민감도 레이블은 세 가지의 요소, 즉 필수적으로 포함되는 계층 레벨 (hierarchical level), 0개 또는 그 이상의 수평적 컴파트먼트 (horizontal compartment), 0개 또는 그 이상의 부모 자식 그룹 (parent child group)으로 구성됩니다. 예를 들어 Secret:ProjectAthens:ExecOnly 민감도 레이블은 Secret 레벨과, ProjectAthens 컴파트먼트, 그리고 ExecOnly 그룹으로 구성됩니다. 실제 환경에서는 레벨 컴포넌트만이 사용되는 경우도 많습니다.

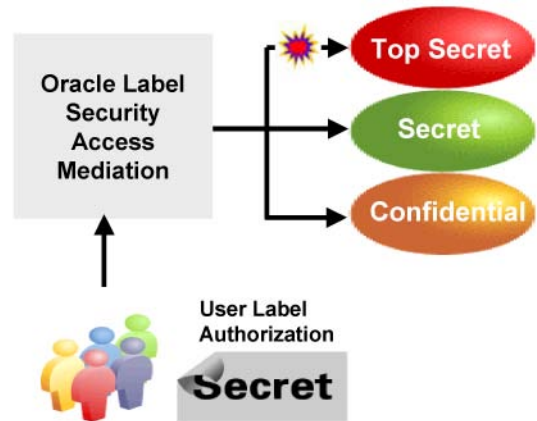


그림. 1 Oracle Label Security 개요

Oracle Database Vault와의 통합

Oracle Database Vault과 함께 적용하는 경우, 민감도 레이블은 컴플라이언스 요구 사항의 해결을 위한 멀티-팩터 권한 할당 (multi-factor authorization)에서 매우 유용하게 활용될 수 있습니다. 예를 들어, Oracle Database Vault 커맨드 룰에서 사용자 레이블 권한을 이용하여 데이터베이스, SQL 커맨드, 애플리케이션 테이블에 대

ORACLE LABEL SECURITY

관련 제품:

보안, 개인정보보호, 컴플라이언스 등의 요구 사항에 대응하는 오라클 제품이 아래와 같습니다:

- Oracle Database Vault
 - 애플리케이션 데이터를 DBA 및 슈퍼 유저로부터 보호
 - 애플리케이션 및 데이터베이스에 대한 투명한 액세스 컨트롤
 - 데이터베이스에 대한 무단 변경 시도를 차단
- Oracle Advanced Security
 - 애플리케이션의 SQL 코드를 전혀 수정하지 않고 투명한 데이터베이스 암호화 지원
 - AES 256 지원
 - 강력한 인증 기능
 - 네트워크 암호화
- Oracle Secure Backup
 - 테이프 백업 수행 과정에서 데이터베이스 및 파일 시스템 데이터를 암호화
- Oracle Recovery Manager(RMAN)와의 통합 지원 및 최대 256 비트 AES 암호화 지원

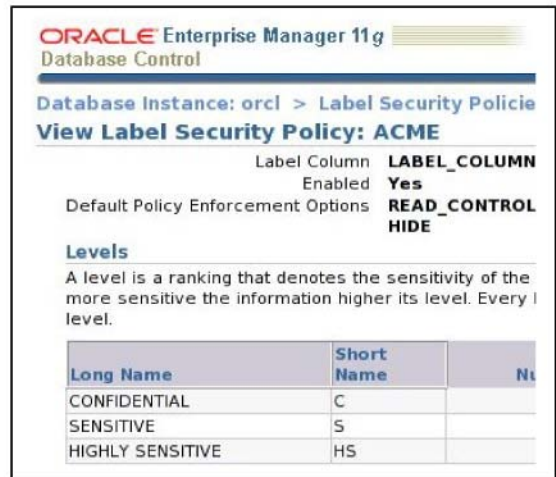
한 액세스를 컨트롤하는 것이 가능합니다. 이처럼 강력한 기능을 포함하는 Label Security의 개념을 활용하여 고전적인 로우 레벨 액세스 컨트롤의 한계를 뛰어넘을 수 있습니다.

유연성과 적응성

Oracle Label Security는 로우 레벨 액세스 컨트롤을 위한 다양한 실행 옵션을 제공합니다. 정책은 읽기 작업에만, 업데이트 작업에만, 또는 두 가지 작업 모두에 적용될 수 있습니다. 사용자 레이블 권한에는 최대 읽기 레이블(maximum read label), 디폴트 쓰기 레이블(default write label), 디폴트 세션 레이블(default session label) 등이 포함됩니다. 최대 읽기 레이블은 사용자가 접근할 수 있는 최대 데이터 민감도 레이블을 의미합니다. 디폴트 쓰기 레이블은 사용자의 INSERT 작업에 할당되는 디폴트 데이터 민감도 레이블입니다. 디폴트 세션 레이블은 사용자가 데이터베이스에 연결할 때 할당되는 디폴트 민감도 레이블입니다. 이 값은 최대 읽기 레이블과 같거나 작아야 합니다. 특수 권한(special authorization)을 통해, 사용자 또는 저장 프로시저에 할당된 사용자 레이블 권한에 관계없이 전체 데이터에 대한 읽기 또는 업데이트 작업을 허용할 수도 있습니다. 특수 권한은 패치, 유지보수 작업에서 유용하게 활용됩니다. 대규모 사용자 애플리케이션을 위한 프록시 기능은 Label Security 프로파일 액세스 권한(profile access authorization)을 통해 제공되며, 애플리케이션 사용자를 위한 레이블 권한을 가정할 수 있게 합니다. Label Security 정책에 SQL 구문의 'where' 조건을 추가하여 민감도 레벨 이외의 액세스 컨트롤 규칙을 할당할 수 있습니다. 레이블 권한은 데이터베이스 사용자가 아닌 사용자 계정도 할당이 가능함을 참고하시기 바랍니다. 이 모델은 공통 애플리케이션 아키텍처를 지원합니다.

단순화된 관리성

Oracle Label Security는 사용이 편리한 정책 기반 관리 모델을 제공합니다. 정책은 민감도 레이블, 레이블 권한, 보호 대상 오브젝트의 논리적 컨테이너 역할을 합니다. 동일한 데이터베이스에 여러 가지 정책이 설정될 수 있습니다. Oracle Identity Management와의 통합 기능을 이용하면 정책과 사용자 레이블 권한을 중앙 집중적으로 관리할 수 있습니다. Enterprise Manager Label Security 콘솔 이외에도 Label Security API가 별도로 제공됩니다.



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.