

ORACLE ADVANCED SECURITY

주요 혜택 및 기능

ORACLE 11g DATABASE

주민등록번호, 신용카드번호 등의 기밀 데이터를 투명하게 암호화

- 테이블스페이스 암호화를 통해 전체 애플리케이션 테이블을 투명하게 암호화
- RMAN 및 TDE를 이용한 데이터베이스 백업본의 암호화
- SQL*Net 네트워크 트래픽의 투명한 암호화
- 강력한 인증 기능 (Kerberos, PKI, RADIUS)
- 컴플라이언스 요건의 준수 (PCI, SOX, HIPAA)
- 표준 지원 (3DES 168, AES 256, SHA-1, x.509v3, PKCS #7/10/11/12, TLS 1.0)

Oracle Advanced Security는 네트워크, 백업 미디어, 또는 데이터베이스의 기밀 데이터를 불법적인 유출 시도로부터 보호함으로써 컴플라이언스 요구 사항을 준수할 수 있도록 합니다. Oracle Advanced Security의 Transparent Data Encryption(TDE) 기능은 업계 선두의 암호화 기술을 구현하고 있으며, 기존 애플리케이션 코드를 전혀 수정하지 않고도 중요한 데이터를 암호화할 수 있습니다.

Transparent Data Encryption

Oracle Advanced Security의 Transparent Data Encryption(TDE)은 운영체제의 해킹 또는 하드웨어, 백업 미디어의 도난으로 인한 데이터의 유출을 방지하기 위한 강력한 암호화 솔루션입니다. TDE를 이용하여 주민등록번호, 신용카드번호와 같은 고객의 개인 정보를 보호하고 PCI 요건을 준수할 수 있습니다. 관리자는 간단한 ALTER TABLE 명령만으로 기존 애플리케이션 테이블의 데이터를 쉽게 암호화할 수 있습니다.

```
SQL> alter table customers modify (credit_card_number encrypt)
```

다른 대부분의 데이터베이스 암호화 솔루션과 달리, TDE는 기존 애플리케이션에 완전히 투명하게 적용되며 트리거, 뷰, 또는 애플리케이션을 전혀 변경할 필요가 없습니다. 데이터는 디스크에 저장

되는 과정에서 투명하게 암호화되며, 정상적인 인증 및 권한 할당을 거친 애플리케이션 사용자가 읽기를 시도할 때 역시 투명하게 복호화됩니다. 인증 과정에서는 사용자가 애플리케이션 테이블에 대한 SELECT, UPDATE 권한을 가지고 있는지 확인하고 Database Vault, Label Security,

Virtual Private Database 정책에 대한 확인 작업을 거칩니다. 기존의 데이터베이스 백업 루틴은 모두 정상적으로 실행 가능하며, 데이터는 백업본에 암호화된 상태로 보존됩니다. TDE와 Oracle RMAN을 함께 사용하여 전체 데이터베이스 백업에 암호화를 적용하는 것 또한 가능합니다.

테이블스페이스 암호화

Oracle Database 11g의 Oracle Advanced Security는 테이블스페이스 암호화 기능을 지원합니다. Enterprise Manager 또는 커맨드라인을 통해 테이블스페이스를 최초 생성하는 과정에서 테이블스페이스 파일을 파일 시스템 상에서 암호화할 수 있는 옵션이 제공됩니다. 테이블스페이스에 INSERT 명령 또는 datapump 유틸리티

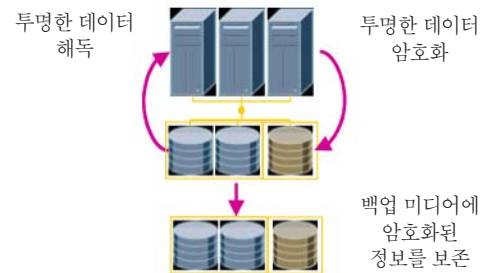


그림 1. Transparent Data Encryption 개요

ORACLE ADVANCED SECURITY

관련 제품:

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

- Oracle Database 10g Release 2 – Oracle Database Vault
 - 애플리케이션 데이터를 DBA 및 수퍼 유저로부터 보호
 - 애플리케이션 및 데이터베이스에 대한 접근 통제
 - 데이터베이스에 대한 무단 변경 시도를 차단
- Oracle Label Security
 - 레이블 기반 액세스 컨트롤
 - 멀티-레벨 보안
 - 기밀 데이터의 보호
 - 레이블 팩터 (label factor)를 통한 Oracle Database Vault와의 통합
 - Common Criteria Evaluation EAL4 인증 획득
- 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

를 통해 새로운 데이터가 추가되면, 전체 테이블이 투명하게 암호화됩니다. 암호화된 테이블스페이스의 데이터 블록에 대한 해독 작업은 사용자에게 투명하게 수행됩니다.

하드웨어 보안 모듈

Oracle Database 11g Release 1에서 TDE의 기능이 개선되어, TDE 마스터 암호화 키를 하드웨어 보안 모듈(HSM) 디바이스에 저장하는 것이 가능해졌습니다. 따라서 TDE 마스터 키의 보호 수준을 더욱 향상시킬 수 있습니다. Oracle Database 11g Release 1는 PKCS#11 인터페이스를 통해 HSM 디바이스와의 커뮤니케이션을 수행합니다. 기존의 월렛(wallet) 기반 마스터 키 저장 메커니즘 또한 계속적으로 지원됩니다.



그림 2. TDE 키 관리 아키텍처

전송중인 데이터의 보호

Oracle Advanced Security는 네이티브 네트워크 암호화, SSL 기반 암호화 등을 이용하여 오라클 데이터베이스를 중심으로 하는 모든 커뮤니케이션을 보호하기 위한, 포괄적이고 편의성이 뛰어난 솔루션입니다. 퍼블릭 키 인프라스트럭처(PKI)를 구현한 비즈니스 환경을 위한 SSL 기반 암호화 및 인증이 지원됩니다. TLS 1.0 프로토콜(AES Cipher Suite 포함)은 Oracle Database 10g Release 1부터 지원되기 시작했습니다. 암호화가 비활성화된 클라이언트의 연결을 거부하거나, 또는 (유연성 보장을 위해) 암호화된 연결을 지원하도록 설정하는 것이 가능합니다. Oracle Network Configuration 관리 툴을 이용하면 네트워크 보안 구성 작업을 단순화하고 애플리케이션을 전혀 변경하지 않은 상태에서도 쉽게 네트워크 암호화 환경을 구축할 수 있습니다.

패스워드 기반 인증을 보다 강력한 인증 방식으로 대체

Oracle Advanced Security는 Kerberos, PKI, RADIUS 등의 강력한 인증 메커니즘을 지원합니다. 인증서 폐기 목록(Certificate Revocation List)을 파일 시스템, Oracle Internet Directory 또는 CDP(CRL Distribution Point)에 저장할 수 있습니다. PKCS #11 표준 기반의 스마트 카드 지원 또한 가능합니다. 인증서는 PKCS #12 표준을 이용하여 공유될 수 있습니다.