ORACLE ADVANCED SECURITY

BENEFICIOS Y CARACTERÍSTICAS CLAVE

ORACLE DATABASE 11g

- Encriptación transparente de SSN, números de tarjeta de crédito y demás datos privados
- Encriptación transparente de todas las tablas de aplicaciones con encriptación del espacio de tabla
- Encriptación de todos los backups de la base de datos con RMAN y TDE
- Encriptación transparente del tráfico de red SQL*Net
- Posibilitar autenticaciones rigurosas (Kerberos, PKI, RADIUS)
- Cumplimiento regulatorio - PCI, SOX, HIPAA
- Compatible con estándares (3DES 168, AES 256, SHA-1, x.509v3, PKCS #7/10/11/12, TLS 1.0)

Oracle Advanced Security ayuda a los clientes a cumplir con los requisitos del cumplimiento regulatorio al proteger los datos sensibles – en la red, en los medios de backup o dentro de la base de datos – de la divulgación no autorizada. Oracle Advanced Security Transparent Data Encryption brinda a las industrias capacidades más avanzadas de encriptación para proteger la información sensible sin la necesidad de realizar cambios en la aplicación existente.

Transparent Data Encryption

Oracle Advanced Security Transparent Data Encryption (TDE) brinda buenas soluciones de encriptación para proteger los datos sensibles contra el acceso no autorizado al sistema operativo o contra el robo de hardware o medios de backup. TDE ayuda a cumplir con los requisitos de privacidad y PCI al proteger la información personalmente identificable, como números de seguridad social y números de tarjetas de crédito. Con un simple comando *alter table*, un administrador puede encriptar los datos sensibles dentro de una tabla existente de aplicaciones.

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

A diferencia de la mayoría de las soluciones de encriptación de base de datos, TDE es totalmente transparente para las aplicaciones existentes, y no es necesario ningún cambio en las aplicaciones, triggers ni vistas. Los datos se encriptan de manera transparente cuando se escriben en el disco y se decodifican después de que un usuario de aplicaciones se haya autenticado exitosamente, y haya pasado todos los controles de autorización. Los controles de autorización incluyen la verificación de que el usuario cuenta con los privilegios *select* y *update* necesarios en la tabla de aplicación y el control de las políticas de cumplimiento de Database Vault, Label Security y Virtual Private Database. Las rutinas existentes para el backup de base de datos seguirán funcionando, y los datos permanecerán encriptados en el backup. Para la encriptación de backups completos de base de datos, TDE puede utilizarse junto con Oracle RMAN.

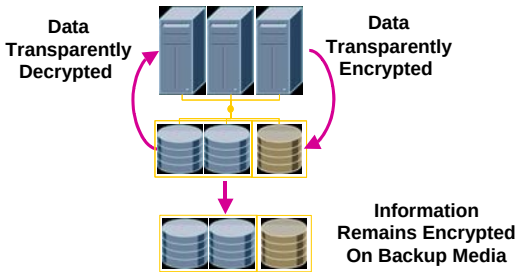

Fig 1. Transparent Data Encryption Overview

Encriptación del Espacio de Tabla

Oracle Advanced Security en Oracle Database 11g versión 1 incluye el soporte de la encriptación de espacios de tabla. Cuando se crea un espacio de tabla mediante Enterprise Manager o en la

ORACLE ADVANCED SECURITY

PRODUCTOS RELACIONADOS

Los siguientes productos ofrecen seguridad adicional para ayudar a cumplir con los requisitos regulatorios, de privacidad y seguridad.

- Oracle Database 10g versión 2 – Oracle Database Vault
  - Protege los datos de las aplicaciones de los DBA y los usuarios privilegiados
  - Controla el acceso a las aplicaciones y bases de datos
  - Protege contra los cambios en la Base de Datos
- Oracle Label Security

Control de acceso basado en etiquetas

  - Seguridad de niveles múltiples
  - Protección de datos sensibles
  - Integrado con Oracle Database Vault mediante factores de etiqueta
  - Evaluación de Criterio Común en EAL4
- Oracle Secure Backup
  - Encriptación de datos del sistema de archivo y la base de datos durante el backup de cinta
  - Integrado con Oracle Recovery Manager (RMAN) y soporta AES de hasta 256 bits

línea de comando, aparece una opción para especificar que el archivo se encripte en el sistema de archivos. Cuando se agregan nuevos datos en el nuevo espacio de tabla utilizando el comando *insert* o bombeo de datos, se encriptarán tablas enteras en forma transparente. Cuando la base de datos lee bloques de datos desde el espacio de tabla encriptado, descifrará transparentemente los bloques de datos.

Módulos para Seguridad de Hardware

TDE ha sido mejorado en Oracle Database 11g versión 1 para soportar el almacenamiento de la clave de encriptación maestra TDE externamente en un dispositivo para módulos de seguridad de hardware (hardware security module - HSM). Esto ofrece un nivel aún mayor de seguridad para proteger la clave maestra TDE. Oracle Database 11g versión 1 se comunica con el dispositivo HSM utilizando la interface PKCS#11. Se seguirá respaldando el mecanismo existente de almacenamiento basado en wallet para la clave maestra.

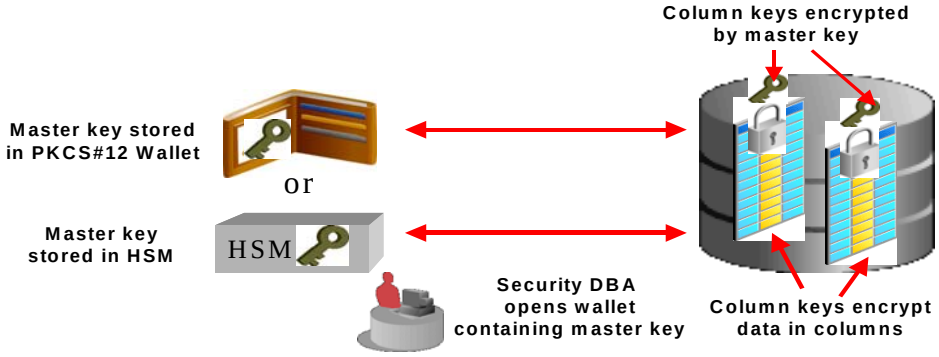

Fig 2. TDE Key Management Architecture

Gran Protección para Datos en Tránsito

Oracle Advanced Security brinda una solución fácil de implementar y completa para proteger todas las comunicaciones desde y hacia Oracle Database, brindando tanto encriptación de red como encriptación SSL. La autenticación y encriptación SSL se encuentran disponibles para empresas que han implementado la Infraestructura de Clave Pública (Public Key Infrastructure). El soporte del protocolo TLS 1.0 (incluidas las suites de código AES) fue introducido en Oracle Database 10g versión 1. Oracle Database puede configurarse para rechazar conexiones de clientes con encriptación deshabilitada, u opcionalmente permitir conexiones no encriptadas para lograr flexibilidad de implementación. La configuración de la seguridad de red se ve simplificada utilizando la herramienta de administración Oracle Network Configuration, lo cual permite a las empresas implementar fácilmente la encriptación de red, ya que no se requieren cambios en la aplicación.

Una Sólida Autenticación Reemplaza la Autenticación Basada en Contraseñas

Oracle Advanced Security ofrece soporte de base de datos para los sólidos servicios de autenticación Kerberos, PKI y RADIUS. Las Listas de Revocación de Certificados se pueden almacenar en el sistema de archivo, Oracle Internet Directory o mediante el uso de Puntos de Distribución CRL. Se ofrece soporte de tarjetas inteligentes utilizando el estándar PKCS #11. Las credenciales se pueden compartir utilizando el estándar PKCS #12.