ORACLE ADVANCED SECURITY

- Transparently encrypt data without application changes
- Built-in key management
- Encrypt entire application tables or individual columns
- Encrypt database exports and RMAN backups
- Encrypt Oracle SQL*Net network traffic
- Fully interoperable with Oracle Advanced Compression technologies
- Fully Interoperable with Oracle GoldenGate 11.1.1.1
- Exadata X2 'Smart Scan' and EHCC support
- Cryptographic acceleration with AES-NI on Intel® XEON® 5600
- Industry standards – AES, 3DES, PKCS#11,PKCS#12, X.509v3

Oracle Advanced Security helps customers address regulatory compliance requirements by protecting sensitive data on the network, on storage media and within the database from unauthorized disclosure. Transparent Data Encryption, a major component of Oracle Advanced Security, provides the industry's most advanced database encryption solution for protecting sensitive information without requiring changes to applications.

Overview

Oracle Advanced Security is an option to the Oracle Database 11g Enterprise Edition that helps address privacy and regulatory requirements including the Payment Card Industry Data Security Standard (PCI), Health Insurance Portability and Accountability Act (HIPAA), and numerous breach notification laws. Oracle Advanced Security provides data encryption and strong authentication services to the Oracle database, safeguarding sensitive data against unauthorized access from the network and the operating system. It also protects against theft, loss, and improper decommissioning of storage media and database backups.

Transparent Data Encryption

Transparent data encryption (TDE) encrypts data before it is written to storage and automatically decrypts data when reading it from storage without any changes to existing applications – no triggers, views or other costly changes. Access controls that are enforced by the Oracle database, including object grants, roles, virtual private database and Oracle Database Vault, still remain in effect.
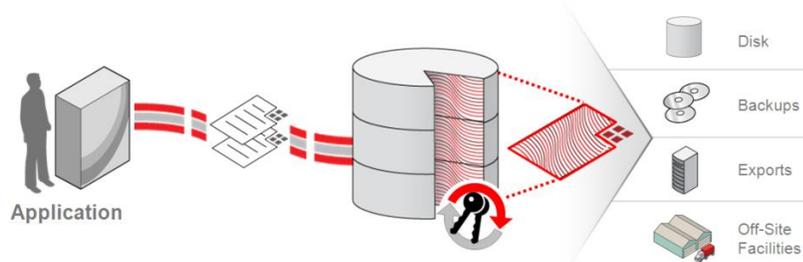
TDE supports two modes: tablespace encryption and column encryption. TDE *tablespace* encryption, introduced with Oracle Database 11g, provides an efficient solution for encrypting entire application tables. TDE tablespace encryption fully supports Exadata X2 including Smart Scan and Hybrid Columnar Compression (EHCC). Starting with Oracle Database 11.2.0.2, TDE tablespace encryption automatically utilizes the hardware acceleration of the Intel® Xeon® 5600 CPUs with AES-NI, enabling Oracle Database 11g to encrypt and decrypt data up to 10 times faster on Intel® platforms, including the Oracle Exadata Database Machine. TDE *column* encryption, introduced with Oracle Database 10g Release2, provides an efficient solution for encrypting individual data elements such as credit card and social security numbers. For TDE column and tablespace encryption, frequently

ORACLE®

accessed data blocks are cached in memory in the same manner as traditional non-encrypted data blocks. This efficient use of native database performance optimizations enables TDE to minimize overhead. TDE tablespace and column encryption also can be used in combination within the same database for hybrid encryption solutions.

Key Management

Oracle Advanced Security provides a built-in, two-tier key management architecture, consisting of a master encryption key and one or more data encryption keys. The TDE master encryption key is used to encrypt and protect the data encryption keys. The master encryption key resides outside of the database in the Oracle Wallet.

Strong Protection for Data In Transit

Oracle Advanced Security provides standards-based network encryption for protecting all communication to and from the Oracle Database. Connections can be rejected from clients that have encryption turned off. No changes to existing applications are required, allowing businesses to easily deploy network encryption.

Strong Authentication Replaces Password Based Authentication

Oracle Advanced Security provides strong authentication to the database using Kerberos, PKI or RADIUS. Oracle Advanced Security interoperates with the Microsoft Kerberos and MIT Kerberos v5. With Oracle Advanced Security, customers can require their users to plug-in a Smart Card (CAC, HSPD-12) as part of their SSL-based authentication to the Oracle Database.

Strong Protection for Database Backups

Data encrypted with TDE remains encrypted when the database files are backed-up to disk with Oracle RMAN. Oracle RMAN can also use TDE during the backup process to encrypt the entire database backup, including the SYSTEM and SYSAUX tablespaces. In addition, Oracle RMAN compression and TDE can be used together to generate backups that are both compact and secure.

Application Certification with Transparent Data Encryption

Oracle Advanced Security TDE is certified with many applications, including Oracle E-Business Suite, Oracle PeopleSoft Enterprise, Oracle Siebel CRM, Oracle JD Edwards EnterpriseOne and SAP.

Contact Us

For more information about Oracle Advanced Security, visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

ORACLE®