Informe Técnico sobre Oracle Advanced Security

Informe Ejecutivo de Oracle

Junio de 2007

ORACLE

Informe Técnico sobre Oracle Advanced Security

INTRODUCCIÓN **3**
GENERALIDADES SOBRE LA ENCRIPTACIÓN DE ORACLE DATABASE **3**
ENCRIPTACIÓN TRANSPARENTE DE DATOS **4**
Beneficios de la Encriptación Transparente de Datos 5
Generalidades sobre la Administración de Claves 5
PASOS DE IMPLEMENTACIÓN **6**
Activar la Clave Maestra **7**
Abrir Oracle Wallet 7
Cambiar la Clave Maestra 7
Cambiar la Contraseña Wallet 7
Identificar datos sensibles **7**
Verificar el soporte TDE de tipos de datos **7**
Controlar el Uso de Claves Externas 8
Encriptación de Datos mediante el Uso de TDE **8**
Cambiar la clave de Tablas/Columnas 8
Mejores Prácticas al Encriptar por Primera Vez los Datos 8
ENCRIPTACIÓN DE BACKUP CON RMAN **9**
Modos de Encriptación RMAN **9**
Encriptación Transparente de Backups 9
Backups Encriptados por Contraseña 10
Backups Encriptados con modo dual 10
MEJORAS EN LA ENCRIPTACIÓN TRANSPARENTE DE DATOS **10**
Soporte de Tipos de Datos Adicionales 10
Encriptación del Espacio de Tabla 10
Protección de Clave Maestra para Módulos de Seguridad de Hardware (HSM) 10
Encriptación DataPump 11
Soporte de Oracle Streams y Logical Standby 11
ENCRIPTACIÓN DE RED **11**
Encriptación Estándar del Sector e Integridad de Datos 11
SSL 12
Seguridad JDBC 12
Fácil Configuración, Ningún Cambio en sus Aplicaciones 12
Buenos Servicios de Autenticación para Oracle Database 10g 12
Autenticación Kerberos **13**
Mejoras en Kerberos 13
Soporte PKI **13**
Soporte PKCS#12 13
Soporte PKCS#11, Tarjetas Inteligentes/Módulos de Seguridad de Hardware 14
Autenticación PKI para Usuarios Empresariales de Oracle Database 10g 14
Wallets Almacenadas en Oracle Internet Directory 14
Soporte de Certificados Múltiples 14
Sólida Encriptación Wallet 14
RADIUS (Servicio Dial-in para Usuarios Remotos) **14**
RESUMEN **16**

Informe Técnico sobre Oracle Advanced Security 11g

INTRODUCCIÓN

Operar en el actual entorno global de negocios plantea varios desafíos de seguridad y cumplimiento. Los beneficios económicos de la subcontratación deben relacionarse con protecciones adecuadas para resguardar la propiedad intelectual y la información relacionada con la privacidad. En los últimos años, se han producido varios incidentes de robo de identidad y fraudes de tarjetas de crédito, lo cual dio como resultado daños multimillonarios. La protección contra este tipo de amenazas requiere soluciones de seguridad transparentes en diseño. Las universidades y organizaciones de salud están fortaleciendo la seguridad en cuanto a la información personalmente identificable (PII), como los números de seguridad social, mientras los minoristas trabajan para cumplir con los requerimientos PCI-DSS. Oracle Advanced Security brinda una seguridad transparente, basada en estándares, que protege los datos en la red, en el disco y en los medios de backup.

GENERALIDADES SOBRE LA ENCRIPTACIÓN DE ORACLE DATABASE

La encriptación es un componente clave del principio defensa-en-profundidad y es importante para proteger los datos en tránsito y en reposo. Oracle primero introdujo las API para la encriptación de base de datos en Oracle8i. Actualmente, las API para encriptación de base de datos Oracle son utilizadas por muchos clientes para encriptar los datos de aplicaciones sensibles. Lograr la transparencia y utilizar una API de encriptación requiere la incorporación de llamadas de función dentro de la propia aplicación o el uso de triggers de base de datos previamente insertados. También se pueden necesitar visualizaciones de las aplicaciones para decodificar los datos antes de que lleguen a la aplicación. Asimismo, la administración de claves debe manejarse de manera programática.

Oracle Advanced Security Transparent Data Encryption (TDE), primero introducido en Oracle Database 10g versión 2, es la solución más avanzada del sector para la encriptación. TDE ofrece administración clave y transparencia completa de encriptación de datos de aplicaciones sensibles. El proceso de encriptación de base de datos es activado mediante el uso de comandos DDL, eliminando por completo la necesidad de cambios en las aplicaciones, la administración programática de claves, los triggers de base de datos y las visualizaciones.

Característica del paquete	DBMS OBFUSCATION TOOLKIT (Oracle 8i y superior) SE & EE	DBMS CRYPTO (Oracle Database 10g R1 y superior) SE & EE	Oracle Advanced Security Transparent Data Encryption EE (única opción)
Algoritmos criptográficos	DES, 3DES	DES, DES, AES, RC4, 3DES_2KEY(1)	3DES, AES (128, 192 y 256 bits)
Planillas para completar	Sin soporte	PKCS5, ceros	PKCS5(2)
Modos de encadenamiento para el cifrado de bloques	CBC	CBC, CFB, ECB, OFB	CBC(2)
Algoritmos criptográficos *hash*	MD5	SHA-1, MD4(1), MD5(1)	SHA-1(2)
Algoritmos *hash* con clave (MAC)	Sin soporte	HMAC_MD5, HMAC_SH1	No disponible
Generador criptográfico de números pseudoaleatorios	RAW, VARCHAR2	RAW, NUMBER, BINARY_INTEGER	No disponible
Tipos de base de datos	RAW, VARCHAR2	RAW, CLOB, BLOB	Todos menos: OBJ., ADT, LOB

1) Ofrecido para la compatibilidad con versiones anteriores
2) Utilizado internamente, no disponible para desarrolladores

Tabla 1. Generalidades sobre la Encriptación de Oracle Database

ENCRIPTACIÓN TRANSPARENTE DE DATOS

TDE encripta los datos antes de que se escriban en el disco y los decodifica antes de que vuelvan a la aplicación. El proceso de codificación y decodificación es realizado en el nivel SQL, de manera completamente transparente para las aplicaciones y los usuarios. Los backups subsiguientes de los archivos de base de datos en disco o cinta tendrán los datos de aplicaciones sensibles encriptados. En forma opcional, TDE puede utilizarse junto con Oracle RMAN para encriptar toda la base de datos Oracle durante el backup a disco.

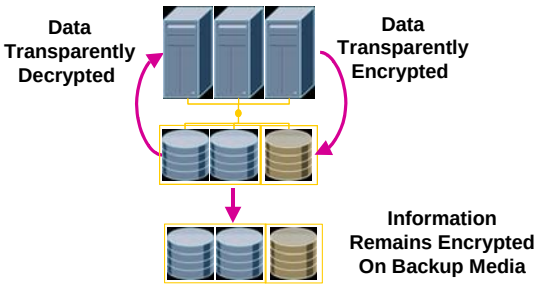

Figura 1. Generalidades sobre la Encriptación Transparente de Datos

Beneficios de la Encriptación Transparente de Datos

1. Administración incorporada de claves
2. Encriptación transparente de columnas de aplicaciones sensibles
3. Encriptación transparente de espacios de tabla **(Nuevo en 11g)**
4. Encriptación transparente de Secure Files/LOBS **(Nuevo en 11g)**
5. Integración con el Módulo de Seguridad de Hardware (HSM) **(Nuevo en 11g)**

Generalidades sobre la Administración de Claves

Automáticamente, TDE crea una clave de encriptación cuando se encripta una columna de la tabla de aplicaciones. La clave de encriptación es específica de la tabla. Si se encripta más de una columna en una sola tabla, la misma clave de encriptación es utilizada para todas las columnas. Cada clave de tabla se almacena en el diccionario de datos Oracle y se encripta utilizando la clave de encriptación maestra TDE. La clave de encriptación maestra se almacena fuera de la base de datos, en Oracle Wallet, un archivo PKCS#12 formateado que se encripta utilizando una contraseña suministrada por un administrador de seguridad designado o por un DBA durante la configuración. La capacidad de almacenar la clave maestra en un dispositivo HSM utilizando la interface PKCS#11 es nueva en Oracle Database 11g Advanced Security.

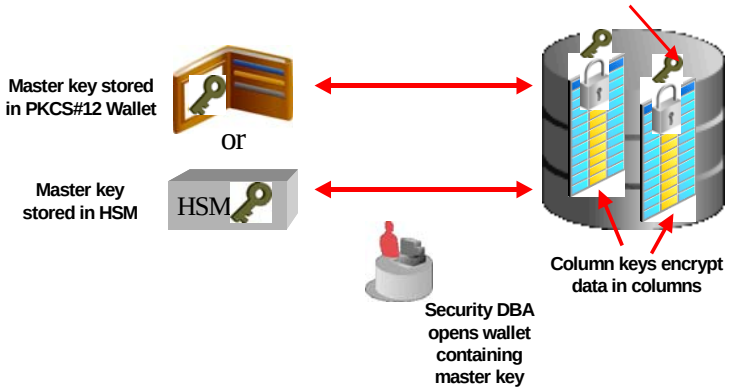

Figura 2. Arquitectura para la Administración de Claves TDE

PASOS DE IMPLEMENTACIÓN

Como TDE es transparente para el código de aplicación existente (no se necesitan *triggers* de base de datos ni vistas), el proceso de encriptación es simple comparado con las soluciones tradicionales de encriptación basadas en API. Los siguientes pasos pueden utilizarse para aplicar TDE:

1. Activar la clave maestra

2. Identificar los datos sensibles que deben encriptarse (datos PII, tarjetas de crédito)

3. Verificar si TDE brinda soporte de los tipos de datos y controlar el uso de claves externas

4. Encriptar los datos sensibles utilizando TDE

Activar la Clave Maestra

Las claves maestras son específicas para cada base de datos. No obstante, cualquier clave maestra puede copiarse en una base de datos secundaria siempre y cuando la clave maestra no haya sido previamente establecida para la base de datos secundaria. La clave maestra debe crearse antes de que una tabla de aplicaciones se encripte. La sintaxis para activar la clave maestra es la siguiente:

```
SQL> alter system set key identified by "password";
```

Este comando crea un *wallet* y utiliza la contraseña para encriptar el *Wallet*, basándose en las recomendaciones del estándar PKCS#5. Oracle Wallet almacena un historial de claves maestras de encriptación ya eliminadas y las pone a disposición cuando los datos encriptados con una clave más antigua se vuelven a leer desde una cinta de backup.

Abrir Oracle Wallet

El *Wallet* que contiene la clave de encriptación maestra debe abrirse antes de que la base de datos pueda desencriptar las claves de tabla para encriptar o desencriptar los datos de las aplicaciones. La base de datos puede comenzar a funcionar sin la necesidad de abrir el *Wallet*. Sin embargo, los intentos de acceder a los datos encriptados generarán un mensaje de error. Cerrar el *Wallet* puede resultar útil durante las operaciones de mantenimiento, cuando se debe otorgar a una persona de soporte el acceso a la base de datos.

Cambiar la Clave Maestra

La clave maestra puede cambiarse generando una vez más el comando "alterar sistema".

```
SQL> alter system set key identified by "password";
```

Cambiar la clave maestra volverá a encriptar las claves de tabla en el diccionario de datos Oracle. El Estándar de Seguridad de Datos PCI 1.1 requiere 'actualizar la clave de encriptación con frecuencia, por lo menos anualmente'. Cambiar la clave maestra volverá a encriptar las claves de columnas utilizando la nueva clave de encriptación maestra; todo ello sin afectar los datos encriptados.

Cambiar la Contraseña Wallet

La contraseña *wallet* puede cambiarse independientemente de la clave de encriptación maestra; solo es utilizada para encriptar el archivo *wallet* en disco. Se puede utilizar Oracle Wallet Manager (que comienza con 'owm' en la línea de comando) o la línea de comando 'orapki'.

Identificar datos sensibles

Identificar los datos relacionados con PII, como los números de seguridad social y de tarjetas de crédito, puede resultar difícil, en especial en una aplicación compleja. Una técnica que puede ser útil es buscar, en el diccionario de datos Oracle, nombres de columnas y tipos de datos frecuentemente utilizados para almacenar dicha información.

```
SQL> select column_name, table_name, data_type from
dba_tab_cols where column_name like '%SOCIAL%' or
column_name like '%SSN%' or column_name like '%SECNUM%' or
column_name like "%SOC%' and owner='<owner>';
```

Verificar el soporte TDE de tipos de datos

TDE brinda soporte de los tipos de datos más comunes utilizados en la base de datos.

VARCHAR2	CHAR	DATE
NUMBER	NVARCHAR2	NCHAR
RAW	RAW	SECUREFILES (LOBS)
BINARY_DOUBLE	BINARY_FLOAT	

Controlar el Uso de Claves Externas

TDE no puede utilizarse para encriptar columnas que se utilizan con una clave externa. Verificar si una columna es utilizada como parte de una clave externa puede lograrse examinando el diccionario de datos Oracle.

```
select A.owner, A.table_name, A.column_name, A.constraint_name
from dba_cons_columns A, dba_constraints B
where
A.table_name = B.table_name and
A.column_name = 'YOURCOLNAME' and
B.constraint_type = 'R';
```

Encriptación de Datos mediante el Uso de TDE

Para encriptar una columna existente:

```
SQL> alter table customers modify (credit_card encrypt);
```

La consistencia de lectura se mantiene mientras se ejecuta la operación de encriptación, permitiendo que las operaciones de selección (lectura) continúen. La operación DML (insertar, actualizar, eliminar) realizada durante la operación de encriptación necesitará una 'redefinición online'.

Crear una nueva tabla con una columna encriptada es fácil. El algoritmo de encriptación por defecto es AES192.

```
SQL> create table billing_information (
first_name varchar2(40)
last_name varchar2(40)
card_number varchar2(19) encrypt using 'AES256');
```

La Encriptación Transparente de Datos trabaja con índices para búsquedas de igualdad, minimizando la carga general implicada en la búsqueda de una columna encriptada.

```
SQL> create index cust_idx on customers (credit_card);
```

Cuando una columna indexada está próxima a ser encriptada, se recomienda primero dar de baja el índice existente, encriptar la columna y, por último, volver a crear el índice.

Cambiar la Clave de Tablas/Columnas

La clave de tablas o columnas, la extensión de la clave y el algoritmo pueden cambiarse independientemente al generar el comando "alterar tabla":

```
SQL> ALTER TABLE employee REKEY;
SQL> ALTER TABLE employee REKEY USING 'AES256';
SQL> ALTER TABLE employee ENCRYPT USING 'AES128';
```

El hecho de cambiar la clave de tablas o columnas hará que se vuelvan a encriptar todos los datos encriptados almacenados en la tabla.

Mejores Prácticas al Encriptar por Primera Vez los Datos

Durante la vida útil de una tabla, los datos pueden fragmentarse, reorganizarse, clasificarse, copiarse y moverse dentro del espacio de tabla; y esto puede dar como resultado copias obsoletas e inaccesibles de datos que residen en bloques de datos no utilizados dentro del archivo de base de datos. Al encriptar una columna existente, solo se encripta la copia 'válida' más reciente, posiblemente dejando atrás versiones más viejas de texto simple. Para minimizar el riesgo relacionado con las copias obsoletas de texto simple creadas antes de la encriptación, Oracle recomienda crear un nuevo espacio de tabla, moviendo la tabla de aplicaciones al nuevo espacio de tabla, y dando de baja el espacio de tabla anterior.

1. Hacer un backup de toda su base de datos

2. Crear un nuevo espacio de tabla especificando un nuevo archivo de datos

3. Encriptar la columna sensible en la tabla original

4. Repetir el paso 3 en todas las tablas que contienen columnas sensibles

5. Mover las tablas del espacio de tabla original al nuevo espacio de tabla

6. Dar de baja el espacio de tabla original utilizando la opción de archivo de datos. De manera opcional, no utilizar la opción '... con archivo de datos' con el comando 'dar de baja al espacio de tabla', pero utilizar el comando 'shred' u otro comando específico de la plataforma para eliminar de manera segura los archivos de datos obsoletos del sistema operativo.

Utilizar un comando del sistema operativo como 'shred' reduce la probabilidad de encontrar copias fantasma del archivo de base de datos, generadas por el sistema operativo o por el *firmware* de almacenamiento.

ENCRIPTACIÓN DE BACKUP CON RMAN

Para una mayor seguridad, los backups RMAN creados como grupos de backup pueden encriptarse utilizando Oracle Advanced Security. Los backups encriptados no pueden leerse si están en manos de personas no autorizadas. Cualquier backup RMAN se puede encriptar como grupo de backup. Sin embargo, los backups de copias de imágenes no pueden encriptarse.

Los backups encriptados son automáticamente desencriptados durante las operaciones de restauración y recuperación, siempre y cuando las claves de decodificación requeridas estén a disposición, por medio de una contraseña suministrada por el usuario o por medio de Oracle Encryption Wallet.

Para utilizar la encriptación RMAN, el parámetro de inicialización COMPATIBLE en la base de datos objetivo debe estar configurado por lo menos en 10.2.0.

Cuando se utiliza el comando *backup backupset* con los grupos de backup encriptados, se realiza un backup de los grupos de backup en su forma encriptada. Debido a que

backup backupset solo copia un grupo de backup ya encriptado al disco o la cinta, no se necesita ninguna clave de decodificación durante una operación *backup backupset*, y los datos no se decodifican nunca durante la operación. El comando *backup backupset* no puede ni encriptar ni desencriptar los grupos de backup.

Si algunas columnas de la base de datos se encriptan utilizando la Encriptación Transparente de Datos, y se realiza un backup de esas columnas utilizando la encriptación de backup, esas columnas se encriptarán por segunda vez durante el backup. Cuando se desenciptan los grupos de backup durante una restauración, las columnas encriptadas vuelven a la forma encriptada original. Si no se especifica ningún algoritmo de encriptación, el algoritmo de encriptación por defecto es AES de 128 bits.

Modos de Encriptación RMAN

RMAN ofrece tres modos de encriptación: modo transparente, modo de contraseña y modo dual. Tanto el modo transparente como el modo dual dependen de Oracle Encryption Wallet.

Encriptación Transparente de Backups

La encriptación transparente puede crear y restaurar backups encriptados sin la intervención del DBA, siempre y cuando la infraestructura para la administración de claves Oracle esté disponible. La encriptación transparente es más adecuada para operaciones de backup diarias, donde los backups se restaurarán en la misma base de datos desde la cual se realizó el backup. La encriptación transparente es el modo por defecto para la encriptación RMAN.

Al utilizar la encriptación transparente, usted primero debe configurar Oracle Encryption Wallet, de acuerdo con lo descrito en la documentación sobre la característica Encriptación Transparente de Datos de Oracle. Después de configurado Oracle Encryption Wallet, los backups encriptados pueden crearse y restaurarse sin la intervención del DBA.

Backups Encriptados por Contraseña

La encriptación por contraseña requiere que el DBA proporcione una contraseña al crear y restaurar los backups encriptados. Restaurar un backup encriptado por contraseña requiere la misma contraseña que fue utilizada para crear el backup. La encriptación por contraseña es útil para los backups que serán restaurados en ubicaciones remotas, pero que deben permanecer seguros en tránsito. La encriptación por contraseña no puede configurarse continuamente. Oracle Encryption Wallet no necesita configurarse si se tiene planeado utilizar la encriptación por contraseña de manera exclusiva.

Si usted se olvida de la contraseña que utilizó para encriptar un backup encriptado por contraseña, no podrá restaurar el backup.

Para utilizar la encriptación por contraseña, utilice el comando SET ENCRYPTION ON IDENTIFIED BY password ONLY de su script RMAN.

Backups Encriptados con modo dual

Los backups encriptados con modo dual pueden restaurarse ya sea de manera transparente o al especificar una contraseña. Los backups encriptados con modo dual son útiles cuando se crean backups que son normalmente restaurados *in situ* utilizando Oracle Encryption Wallet, pero que ocasionalmente necesitan restaurarse en otro sitio, en donde Oracle Encryption Wallet no está disponible.

Al restaurar un backup encriptado con modo dual, usted puede utilizar Oracle Encryption Wallet o una contraseña para la desencriptación.

Si usted se olvida la contraseña que utiliza para encriptar un backup encriptado con modo dual, también pierde su Oracle Encryption Wallet, y no podrá restaurar ese backup.

Para crear grupos de backup encriptados con modo dual, especifique el comando SET ENCRYPTION ON IDENTIFIED BY password de su script RMAN.

MEJORAS EN LA ENCRIPTACIÓN TRANSPARENTE DE DATOS

Oracle Database 11g Advanced Security Transparent Data Encryption incluye varias mejoras importantes.

Soporte de Tipos de Datos Adicionales

Oracle Database 11g Advanced Security Transparent Data Encryption brinda soporte para la encriptación del nuevo Oracle Database 11g SecureFiles. Esto permite la encriptación transparente de imágenes médicas escaneadas, contratos y otros documentos altamente sensibles almacenados en la base de datos.

Encriptación del Espacio de Tabla

Oracle Database 11g Advanced Security Transparent Data Encryption incorpora el soporte de la encriptación de espacios de tabla de la base de datos. La encriptación de espacios de tabla significa que pueden encriptarse tablas completas de aplicaciones de manera transparente. Los bloques de datos se desencriptarán transparentemente a medida que la base de datos acceda a ellos.

Solo pueden encriptarse los nuevos espacios de tabla.

```
SQL> CREATE TABLESPACE securespace
DATAFILE '/home/user/oradata/secure01.dbf' SIZE 150M
ENCRYPTION USING 'AES192' DEFAULT STORAGE(ENCRYPT);
```

Se encriptarán todos los objetos de base de datos creados en el nuevo espacio de tabla. La encriptación del espacio de tabla elimina la restricción de clave externa de la encriptación de columnas y permite realizar escaneos por rango de los datos encriptados.

Protección de Clave Maestra para Módulos de Seguridad de Hardware (HSM)

Para una seguridad incluso mayor, la clave de encriptación maestra puede almacenarse en un dispositivos HSM compatible con PKCS#11, que también permite que múltiples bases de datos o instancias de base de datos en un entorno RAC que comparten los mismos datos encriptados compartan la misma clave de encriptación maestra. Como Oracle se adhiere al estándar PKCS#11, los clientes pueden elegir entre una variedad de proveedores de HSM.

Al realizar la actualización de la encriptación en el nivel de columnas con TDE en Oracle 10g R2 a la encriptación de espacios de tabla en Oracle11g R1, usted necesita realizar una operación de cambio de clave (*rekeying*), lo cual generará una nueva clave de encriptación maestra para las columnas encriptadas *y* una nueva clave de encriptación maestra para la encriptación del espacio de tabla.

Si desea realizar la actualización de una clave de encriptación maestra almacenada en Oracle Wallet a una clave de encriptación maestra en un dispositivo HSM, siga los siguientes pasos:

1.) Cambie la clave de la clave maestra para generar una clave de encriptación maestra en caso de que necesite una más adelante

2.) Cambie el archivo sqlnet.ora a:

```
ENCRYPTION_WALLET_LOCATION=
SOURCE=(METHOD=HSM)
```

3.) SQL> alter set key identified by “<user_id:password>” migrate from <wallet password>

<user_id:password> es la información de autenticación para el dispositivo HSM.

Encriptación DataPump

La encriptación transparente de datos puede utilizarse para encriptar todos los contenidos de salida de Oracle Datapump. Esta es una nueva característica de Oracle Database 11g. Por favor, remítase a la documentación de Oracle Datapump para ver detalles adicionales.

Soporte de Oracle Streams y Logical Standby

Oracle Database 11g Advanced Security TDE brinda soporte de bases de datos standby lógicas y Oracle Streams. Oracle Database 10g Release 2 Advanced Security TDE solo brindaba soporte de bases de datos standby físicas.

ENCRIPTACIÓN DE RED

Oracle Advanced Security protege la privacidad y confidencialidad de los datos de red al eliminar el espionaje de datos, la pérdida de datos, los ataques de intermediarios (*person-in-the-middle*) y de repetición (*replay*). Toda comunicación con una base de datos Oracle puede encriptarse con Oracle Advanced Security. Las bases de datos contienen información extremadamente sensible, y el acceso restringido mediante una estricta autenticación es una de las primeras líneas de defensa. Oracle Advanced Security brinda buenas soluciones de autenticación que aprovechan las estructuras de seguridad existentes de una empresa, con inclusión de Kerberos, Criptografía de Clave Pública, RADIUS y DCE para Oracle Database 10g.

Encriptación Estándar del Sector e Integridad de Datos

Oracle Advanced Security protege todo tipo de comunicación desde y hacia Oracle Database. Las empresas pueden elegir entre utilizar los algoritmos de Oracle Advanced Security para encriptación nativa/integridad de datos, y SSL para proteger los datos de la red. Algunos de los escenarios típicos que requieren encriptación en el nivel de red incluyen:

• El Servidor de Base de Datos está detrás de un firewall, y los usuarios acceden al servidor mediante aplicaciones cliente-servidor

• Se debe encriptar la comunicación entre el servidor de aplicaciones en una DMZ y la Base de Datos que está detrás de un segundo firewall

Los algoritmos de Encriptación Nativa e Integridad de Datos en Oracle Advanced Security no requieren la implementación PKI. Con cada lanzamiento de base de datos, se incorporan algoritmos de encriptación más nuevos a medida que obtienen la aprobación de la industria. La última incorporación es el Estándar de Encriptación Avanzada (AES), un algoritmo mejorado en seguridad y rendimiento sobre DES. El listado completo de algoritmos de Encriptación e Integridad de Datos es

• AES (128, 192 y 256 bits)

• RC4 (40, 56, 128, 256 bits)

• 3DES (2 y 3 claves; 168 bits)

• MD5

• SHA1

La encriptación basada en SSL está disponible para empresas que han elegido utilizar la Infraestructura de Clave Pública en sus implementaciones de IT. Oracle

Advanced Security 10g ha incorporado soporte del protocolo TLS 1.0. Oracle Advanced Security proporciona grupos de cifrado AES con el protocolo TLS 1.0 comenzando en Oracle Database 10g.

SSL

Oracle implementa el protocolo SSL para la encriptación de datos intercambiados entre clientes de base de datos y la base de datos. Esto incluye datos de Oracle Net Services (anteriormente, conocido como Net8), LDAP, JDBC, y el formato IIOP. La encriptación SSL brinda a los usuarios una alternativa del protocolo de encriptación nativo Oracle Net Services que ha sido respaldado en Oracle Advanced Security (anteriormente conocido como Advanced Networking Option) desde Oracle7. Un beneficio de SSL es que es un estándar de Internet de facto, y puede utilizarse con clientes que usan otros protocolos que no sean Oracle Net Services.

En un sistema de tres niveles, el soporte SSL en una base de datos implica que los datos intercambiados entre el nivel medio y la base de datos pueden encriptarse utilizando SSL. El protocolo SSL ha ganado la confianza de los usuarios, y es tal vez el protocolo de encriptación más ampliamente implementado y conocido que se utiliza actualmente. La implementación de SSL por parte de Oracle respalda los tres modos estándar de autenticación, que incluyen la autenticación anónima (Diffie-Hellman), la autenticación servidor-servidor con el uso de certificados X.509, y la autenticación mutua (cliente-servidor) con X.509.

Oracle Application Server también brinda soporte de la encriptación SSL entre clientes livianos (*thin clients)* y Oracle Application Server, así como entre Oracle Application Server y Oracle Data Server. Como en Oracle, se brinda soporte de la autenticación anónima, servidor-servidor y cliente-servidor mediante X.509.

Seguridad JDBC

JDBC es una interface Java estándar del sector que ofrece un estándar Java para conectarse a una base de datos relacional desde un programa Java. Sun Microsystems definió el estándar JDBC, y Oracle Corporation, como proveedor individual, implementa y extiende el estándar con sus propios *drivers* JDBC. Oracle implementa dos tipos de *drivers* JDBC: *Thick JDBC drivers* creados sobre el cliente Oracle Net Services basado en C, y *thin JDBC drivers* (puramente Java) para soportar *applets* descargables.

Como *thick JDBC* utiliza toda la estructura de comunicación Oracle Net Services en el cliente y en el servidor, puede aprovechar los mecanismos existentes de encriptación y autenticación de Oracle Advanced Security. Debido a que *thin JDBC driver* está diseñado para su uso con *applets* descargables utilizados en Internet, Oracle incluye una implementación 100% Java de los algoritmos de encriptación e integridad de Oracle Advanced Security para su uso con clientes livianos (*thin clients*).

Fácil Configuración, Ningún Cambio en sus Aplicaciones

Configurar los parámetros de red para el servidor y/o cliente permite la función de encriptación de red/integridad. La mayoría de las empresas pueden fácilmente adoptar esta tecnología ya que no se requieren cambios en la aplicación.

Buenos Servicios de Autenticación para Oracle Database 10g

El acceso no autorizado a la información es un problema muy antiguo. Hoy en día, las decisiones de negocio están impulsadas por la información que se recopila de la extracción de terabytes de datos. Proteger la información sensible es clave para que una empresa siga siendo competitiva. El acceso a repositorios de datos clave, como Oracle Database 10g, que alojan información valiosa puede otorgarse una vez que los usuarios son identificados y autenticados con precisión. Verificar la identidad de los usuarios incluye recopilar más información que la contraseña y el nombre de usuario. Oracle Advanced Security brinda una capacidad para que las empresas aprovechen sus infraestructuras de seguridad existentes, como Kerberos, la Infraestructura de Claves Públicas (PKI) y RADIUS, a fin de obtener buenos

servicios de autenticación para Oracle Database 11g. Las Listas de Anulación de Certificación pueden almacenarse en el sistema de archivos, Oracle Internet Directory o mediante el uso de Puntos de Distribución CRL.

Los Servidores de Base de Datos Oracle o los Usuarios/Clientes de la Base de Datos tienen la capacidad de utilizar Credenciales PKI almacenadas en Tarjetas Inteligentes u otros Módulos de Almacenamiento de Hardware que utilizan el estándar PKCS#11 del sector. Esto es especialmente útil para los usuarios ya que ofrece acceso *roaming* a la base de datos mediante aplicaciones cliente-servidor o aplicaciones web.

Almacenar credenciales de servidor en un modulo de hardware brinda un nivel adicional de seguridad necesario para algunas implementaciones.

Autenticación Kerberos

Oracle Advanced Security incluye un cliente Kerberos compatible con Kerberos v5 ticket suministrado por cualquier servidor Kerberos compatible con MIT v5 o Microsoft KDC. Las empresas pueden continuar operando en un entorno heterogéneo mediante el uso de la solución Kerberos de Oracle Advanced Security. Una vez registrada una base de datos Oracle con un Servidor Kerberos, y configurada para soportar un Servicio Kerberos, los usuarios empresariales pueden autenticarse en la base de datos sin ninguna complicación adicional. Las organizaciones que ya utilizan un Servidor Kerberos y un adaptador Kerberos de Oracle Advanced Security pueden realizar la migración de sus usuarios externos de bases de datos al directorio para obtener los beneficios de la administración centralizada de usuarios.

Mejoras en Kerberos

Las mejoras de Oracle Database 11g Advanced Security en Kerberos incluyen el soporte de nombres de hasta 2000 caracteres de longitud. Asimismo, Oracle Database 11g Advanced Security ofrece a Kerberos soporte de todos los "reinos", permitiendo a los autores Kerberos de un "reino" autenticar a autores Kerberos de otro "reino".

A continuación, mostramos un ejemplo de la creación de un usuario Oracle externamente autenticado. El nombre de usuario debería corresponder al usuario Kerberos.

```
SQL> CONNECT / AS SYSDBA;
SQL> CREATE USER "KRBUSER@SOMECO.COM" IDENTIFIED EXTERNALLY;
SQL> GRANT CREATE SESSION TO "KRBUSER@SOMECO.COM";
```

Por favor, remítase a la guía de Oracle Advanced Security para administradores a fin de obtener información adicional sobre la configuración de Oracle Database y el cliente para la autenticación Kerberos.

Soporte PKI

El cliente SSL de Oracle Advanced Security puede utilizarse en cualquier PKI compatible con los estándares del sector y aceptar las solicitudes de certificados PKCS7 estándar y emitir certificados X509v3. Oracle Advanced Security brinda un adaptador Entrust que permite que las aplicaciones de negocio aprovechen Entrust PKI con Oracle Database 11g.

Oracle Wallet Manager sigue siendo la herramienta para las solicitudes de certificado y otras tareas de administración de certificados del usuario final. Otros servicios de línea de comando que ayudan en la administración de las Listas de Anulación de Certificación (CRLs) y otras operaciones Oracle Wallet están disponibles en esta versión. Las Listas de Anulación de Certificación publicadas en un servidor LDAP, un sistema de archivos o una URL son respaldadas por la infraestructura SSL de Oracle.

Soporte PKCS#12

Oracle Advanced Security respalda los certificados X.509 almacenados en contenedores PKCS #12, haciendo que Oracle Wallet sea interoperable con aplicaciones de terceros como Netscape Communicator 4.x y Microsoft Internet Explorer 5.x, y ofreciendo portabilidad *wallet* a través de los sistemas operativos. Los usuarios con credenciales PKI existentes pueden exportarlas en formato PKCS#12 y reutilizarlas en Oracle Wallet Manager, y viceversa. PKCS#12 aumenta así la interoperatividad y reduce el costo de la implementación PKI para las organizaciones.

Soporte PKCS#11, Tarjetas Inteligentes/Módulos de Seguridad de Hardware

Oracle Wallet es un contendor de software que contiene la clave privada y otros puntos de confianza de los certificados. Oracle Advanced Security 10g respalda el soporte del estándar del sector PKCS#11. Esto permite que las claves privadas anteriormente almacenadas en el sistema de archivos se creen y almacenen en dispositivos seguros como Módulos de Seguridad de Hardware o Tarjetas Inteligentes disponibles en el mercado.

Autenticación PKI para Usuarios Empresariales de Oracle Database 10g

Desde Oracle8i, Oracle Advanced Security ha respaldado la autenticación para usuarios de directorio de la base de datos Oracle utilizando certificados digitales almacenados en el directorio.

Oracle expande la integración y la interoperatividad PKI a través de:

• Soporte PKCS#11

• Almacenamiento *Wallet* en Oracle Internet Directory

• Múltiples certificados por *wallet*

• Sólida encriptación de *wallet*

• OracleAS Certificate Authority

Wallets Almacenados en Oracle Internet Directory

Oracle Enterprise Security Manager crea *wallets* de usuarios como parte del proceso de inscripción de los usuarios. El *wallet* se almacena en Oracle Internet Directory, u otro directorio compatible con LDAP. Oracle Wallet Manager puede cargar *wallets*—y recuperarlos—en el directorio LDAP.

Almacenar el *wallet* en un directorio centralizado compatible con LDAP brinda soporte para el *roaming* de usuarios, permitiéndoles acceder a sus credenciales desde múltiples lugares o dispositivos, lo cual garantiza una autenticación consistente y confiable de los usuarios, y brinda una administración centralizada de *wallet* a lo largo de todo el ciclo de vida del *wallet*.

Soporte de Certificados Múltiples

Oracle Wallets brinda soporte de múltiples certificados por *wallet*, entre ellos:

• Certificado de firmas S/MIME

• Certificado de encriptación S/MIME

• Certificado de firmas de código

Oracle Wallet Manager versión 3.0 brinda soporte de múltiples certificados para una entidad digital única en un individuo—con múltiples pares de claves privadas en un individuo (cada clave privada puede corresponder a un solo certificado). Esto

permite la consolidación de las credenciales PKI de los usuarios y una administración más segura.

Sólida Encriptación *Wallet*

Las claves privadas asociadas con los certificados X.509 requieren una encriptación sólida, a través de canales seguros. Oracle reemplaza la encriptación DES con Triple DES (3DES) de 3 claves, que es un algoritmo de encriptación mucho más sólido y ofrece una estricta seguridad para Oracle Wallets.

RADIUS (Servicio Dial-in para Usuarios Remotos)

Oracle Advanced Security proporciona un cliente RADIUS que permite a Oracle Database 11g respetar la autenticación y las autorizaciones impuestas por un servidor RADIUS. Esta característica es especialmente útil para empresas interesadas en la autenticación de dos factores, que establece su identidad basándose en lo que usted sabe (contraseña o información del PIN) y en lo que usted tiene (la tarjeta *token*) suministrado por algún fabricante de tarjetas *token*. RADIUS (RFC #2138) es un sistema distribuido que asegura el acceso remoto a servicios de red y se ha consolidado hace mucho tiempo como estándar del sector para el acceso remoto y controlado a las redes. Las credenciales de usuarios RADIUS y la información de acceso están definidas en el servidor RADIUS para permitir que este servidor externo realice los servicios de autenticación, autorización y contabilidad cuando sea necesario.

El soporte de Oracle RADIUS representa una implementación de los protocolos de Cliente RADIUS que permiten a la base de datos brindar autenticación, autorización y contabilidad para usuarios RADIUS. Envía solicitudes de autenticación al servidor RADIUS y actúa de acuerdo con las respuestas del servidor. La autenticación puede producirse en modo sincrónico o asíncrono y forma parte de la configuración Oracle para soporte RADIUS.

Oracle Advanced Security brinda autenticación, respeta las autorizaciones almacenadas en RADIUS y los servicios contables básicos para usuarios RADIUS al acceder a la base de datos Oracle.

RESUMEN

La encriptación es un componente clave del principio defensa-en-profundidad, y Oracle continúa desarrollando soluciones innovadoras para ayudar a los clientes a cumplir con los requerimientos de seguridad, cada vez más exigentes, respecto de la protección de datos PII. Los minoristas pueden utilizar Oracle Advanced Security TDE para cumplir con los requisitos PCI-DSS, mientras las organizaciones de salud y las universidades pueden utilizar TDE para proteger los números de seguridad social y demás información sensible. La encriptación desempeña un rol especialmente importante en el resguardo de datos en tránsito. La encriptación de red de Oracle Advanced Security protege los datos en tránsito de la Intranet frente a las modificaciones y el espionaje de red. Oracle Advanced Security TDE protege los datos sensibles en unidades de disco y medios de backup del acceso no autorizado, ayudando así a reducir el impacto que puede generarse a partir de la pérdida o el robo de medios.

Informe Técnico sobre Oracle Advanced Security
Junio de 2007
Autor: Paul Needham
Coautor: Peter Wahl

Oracle Corporation
Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Consultas:
Teléfono: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Copyright © 2007, Oracle. Todos los derechos reservados.
El presente documento tiene solo fines informativos y su contenido está sujeto a cambios sin que medie notificación alguna. El presente documento puede contener errores y no está sujeto a ninguna otra garantía ni condición, ya sea oral o que se encuentre implícita en la ley, con inclusión de garantías y condiciones implícitas de comerciabilidad o aptitud para un fin específico. En especial, negamos cualquier responsabilidad con respecto al presente documento, el cual no crea obligación contractual alguna, sea en forma directa o indirecta. El presente documento no podrá ser reproducido ni transmitido de ninguna forma ni por ningún medio, sea electrónico o mecánico, con ningún fin, sin que hayamos otorgado previamente nuestro consentimiento por escrito. Oracle es marca registrada de Oracle Corporation y/o sus afiliadas. Otros nombres pueden ser marcas comerciales de sus respectivos propietarios.