Whitepaper Seguridad

Opciones de Seguridad de la BD Oracle 10g R2 (Oracle Database Vault, Oracle Advanced Security Option y Oracle DataMasking)

isvega

19-Abril-2009

Tabla de contenido

Contenido

Introducción 3

ORACLE DATABASE VAULT 4

Cumplimiento de controles 4

Oracle Database Vault y cumplimiento regulatorio 5

Links de interés: 8

ORACLE ADVANCED SECURITY OPTION 9

ORACLE DATAMASKING 14

Introducción

Durante la última década han aparecido diversas regulaciones que dictaminan estrictos controles internos y protección de la información de identificación personal (PII). Constituyen ejemplos de estas regulaciones la ley Sarbanes-Oxley (SOX), el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI), la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA), la Ley de Instrumentos Financieros y Bolsa (Japón), la Ley Basel II y la Directiva de la Unión Europea sobre Privacidad y Comunicaciones Electrónicas en Europa. La continua necesidad de nuevas regulaciones en todo el mundo combinada con la naturaleza cada vez más sofisticada del robo de información requiere de una sólida seguridad de datos.

Si a la fecha Internet ha venido acelerando el desarrollo de nuevas aplicaciones para todos los aspectos del procesamiento de negocios, las regulaciones ahora requieren controles mucho más estrictos para la información delicada, tanto financiera como relacionada con la privacidad. Se requieren soluciones de seguridad transparentes para implementar los controles más estrictos porque la mayoría de las aplicaciones se basan en la seguridad a nivel de aplicación para restringir el acceso a datos delicados. Los conceptos de seguridad como menor privilegio y necesidad de saber se consideraban menos importantes que la escalabilidad y la alta disponibilidad. Los productos de Oracle en seguridad de datos complementan la seguridad a nivel de aplicación permitiendo a las organizaciones minimizar los costos asociados con el cumplimiento de las regulaciones y la implementación de los estrictos controles internos.

Oracle en sus 32 años de existencia ha venido innovando y fortaleciendo su portafolio de soluciones tanto en características embebidas en la Base de datos como funcionalidades con mayor nivel de especialización denominadas opciones, las cuales habilitan la adopción de mejores prácticas y facilitan el cumplimiento de requerimientos asociados con la aplicación de controles, monitoreo y administración de la plataforma Oracle. Este documento centra su atención en las opciones de Cifrado (Oracle Advanced Security Option), Segregación de deberes (Oracle Database Vault) y Mascaramiento de datos en ambientes de desarrollo y test (Oracle DataMasking) y los controles que pueden ser implementados para dar cumplimiento a marcos regulatorios globales y/o locales.

ORACLE DATABASE VAULT

Qué es Oracle Database Vault?

Oracle Database Vault es una opción de seguridad de la BD que se utiliza para proteger datos de la aplicación ante interacciones del DBA, mejora la protección de las estructuras de la base de datos ante cambios no autorizados y cuenta con una amplia variedad de controles de acceso para implementar requerimientos de seguridad de manera dinámica y flexible. Esas Características le ayudan a adherirse a Estándares relacionados con la separación de tareas, cumplimiento regulatorio y control interno. Se configura Oracle Database Vault para Gestionar la seguridad por las instancias individuales de Base de datos. Es posible usar Oracle Database Vault en instalaciones standalone de la BD Oracle Database y en ambientes. Oracle Real Application Clusters (RAC)

La configuración de Oracle Database Vault se hace de manera individual para gestionar la seguridad de cada instancia. Esta opción se instala en las versiones standalone de Oracle Database, en múltiples Oracle homes, y en ambientes de Oracle Real Application Cluster (RAC).

Oracle Database Vault requiere que las versiones de la base de datos sean Oracle 9i (9.2.0.8) Enterprise Edition u Oracle Database 10g Release 2 (10.2.0.3) Enterprise Edition o versiones superiores.

Cumplimiento de controles

Las opciones de seguridad de la base de datos Oracle, dan cumplimiento a un amplio rango de regulaciones y normativas entre las que se destacan las siguientes:

Oracle features and compliance regulations
(SOX, HIPAA, BDSG, European Directive 2002/58/EC)

	Requirement	Oracle DB	Virtual Private Database	Oracle Label Security	Oracle Database Vault	Oracle Advanced Security	Oracle Recovery Manager/ Secure Backup	Oracle Audit Vault	Data Guard	Content DB	Oracle Identity Management	Oracle Real Application Clusters	Oracle AS	Partitioning	EM Configuration Management	ASM	Regulation and Section
1	Data classification	●	●	●	●						●	●					SOX sec.302, 404 Directive Art.7; FDPA 9,14,19 HIPAA 164.308(a)(7)(ii)(E)
2	Data retention	●								●				●		●	SOX sec.103; FDPA 6b, 10, 35 Directive Art.6
3	Data backup						●							●		●	HIPAA 164.310(d)(2)(iv) HIPAA 164.308(a)(7)(ii)(A) SOX sec.409; FDPA 9
4	Recovery	●					●							●			HIPAA 164.308(a)(7)(ii)(B)
5	Integrity	●	●	●	●	●					●						HIPAA 164.312(c)(1);164.312(e)(2)(i) SOX sec.103, 302, 404 FDPA 9,11,14,20,35
6	Encryption	●				●	●						●				HIPAA 164.312(a)(2)(iv) HIPAA 164.312(e)(2)(ii) SOX sec.302, 404; FDPA 6c, 9
7	Identification	●		●							●						HIPAA 164.312(a)(2)(i) SOX sec.302, 404 Directive Art.6, 7, 9; FDPA 9
8	Authentication	●		●	●	●					●						HIPAA 164.312(d) SOX sec.302, 404 Directive Art.6, 7, 9; FDPA 9
9	Authorization	●	●	●							●						SOX sec.302, 404 Directive Art.6, 7, 9; FDPA 5, 9, 14
10	Access control	●	●	●	●						●		●				HIPAA 164.312(a)(1) SOX sec.302, 404 Directive Art.6, 7, 9; FDPA 9
11	Fine-grained access control	●	●	●													HIPAA 164.312(a)(1) SOX sec.302, 404
12	User account management and review of privileges	●		●							●				●		HIPAA 164.308(a)(3)(ii)(C) SOX sec.302, 404
13	Password management	●									●						HIPAA 164.308(a)(5)(ii)(D)
14	Least privilege principle	●	●	●	●												HIPAA 164.308(a)(4)(ii)(A) SOX sec.302, 404 Directive Art.6, 7, 9; FDPA 14
15	Segregation of duties				●												SOX sec.302, 404 Directive Art.6, 7, 9; FDPA 14
16	Monitoring for violation and security activity report (*fine grained auditing*)	●		●				●									HIPAA 164.312(b) HIPAA 164.308(a)(5)(ii)(C) SOX sec.302, 404 Directive Art.9 FDPA 4g, 11, 42
17	Secure communication					●							●				HIPAA 164.312(e)(1) SOX sec.302, 404 Directive Art.5; FDPA 9, 15
18	Audit trails	●		●				●					●				HIPAA 164.312(b) SOX sec.302, 404; FDPA 9,11,14,15,20,35
19	Availability	●							●			●		●		●	HIPAA 164.312(a)(2)(ii) SOX sec.409; FDPA 14, 38
20	Operations logs	●						●					●				SOX sec.103, 302, 404 FDPA 9,20,35

Source: Master Thesis "Secure Enterprises on Oracle-based Infrastructure from Distributed and Centralized Perspectives", Violeta Salogub, Technische Universität Hamburg Harburg

Oracle Database Vault y cumplimiento regulatorio

Los reinos definidos en Oracle Database Vault, Características para segregar deberes, el uso de reglas de comandos y el uso de factores son aplicables para reducir el riesgo mapeando los requerimientos expresos en regulaciones de alcance mundial. Regulaciones tales como Sarbanes-Oxley (SOX), Healthcare Insurance Portability and Accountability Act (HIPAA), Basel II y PCI tienen requerimientos comunes que incluyen el uso de controles internos, separación de deberes y control fuerte para el acceso a información sensible del negocio. Mientras muchos requerimientos encuentran en regulaciones tales como SOX y HIPAA son Iniciativas de naturaleza procedimental, se requiere de las soluciones técnicas para mitigar esos riesgos asociados con ítems tales como modificaciones no autorizadas de los datos y accesos inapropiados.

Oracle Database Vault (DBV) and Regulations		
Regulation	**Requirement**	**Does DBV Mitigate This Risk?**
Sarbanes-Oxley Section 302	Unauthorized changes to data	**Yes**
Sarbanes-Oxley Section 404	Modification to data, Unauthorized access	**Yes**
Sarbanes-Oxley Section 409	Denial of service, Unauthorized access	**Yes**
Gramm-Leach-Bliley	Unauthorized access, modification and/or disclosure	**Yes**
HIPAA 164.306	Unauthorized access to data	**Yes**
HIPAA 164.312	Unauthorized access to data	**Yes**
Basel II – Internal Risk Management	Unauthorized access to data	**Yes**
CFR Part 11	Unauthorized access to data	**Yes**
Japan Privacy Law	Unauthorized access to data	**Yes**
PCI – Requirement 7	Restrict access to cardholder data by business need-to-know	**Yes**
PCI – Requirement 8.5.6	Enable accounts used by vendors for remote maintenance only during the time period needed	**Yes**
PCI – Compensating Controls for Requirement 3.4	Provide ability to restrict access to cardholder data or databases based on the following criteria:	**Yes**
	• IP address/Mac address • Application/service • User accounts/groups	
PCI - Requirement A.1: Hosting providers protect cardholder data environment	Ensure that each entity only has access to own cardholder data environment	**Yes**

Table 1. Oracle Database Vault and Regulations Overview

Sarbanes Oxley Section 404

Para la regulación Sarbanes Oxley se aplican las mejores prácticas de Oracle para el aseguramiento de la base de datos cumpliendo con los siguientes requerimientos:

- Bloqueo y expiración de cuentas por defecto
- Designar una cuenta específica de BD para la creación de usuarios
- Database Vault
- Usar un nuevo almacén externo para contraseñas donde sea posible realizar procesos en lotes.

- Asignar una cuenta específica de BD para la administración de todas las políticas VPD (Virtual Private Database) que se tienen o se planean crear.
- Designar una cuenta específica de BD para Gestionar todas las políticas FGA que se tienen o se planean crear.

Limitar conectividad como SYSDBA donde sea posible

- Oracle está en el proceso de eliminar la dependencia de conexiones SYSDBA (en versiones 11g y superior)
- Comenzar usando SYSOPER para operaciones shutdown / Startup.

Auditoría de Base de datos

- Auditar operaciones del **sys**

- Activar auditoria granular fina para tablas sensibles
- Activar auditoria estándar
- Considerar cuentas no propietarias al mínimo si su preocupación es desempeño.
- Auditar todas las sentencias DDL
- Integrar con la solución Oracle Audit Vault

Enterprise Manager Configuration Scanning

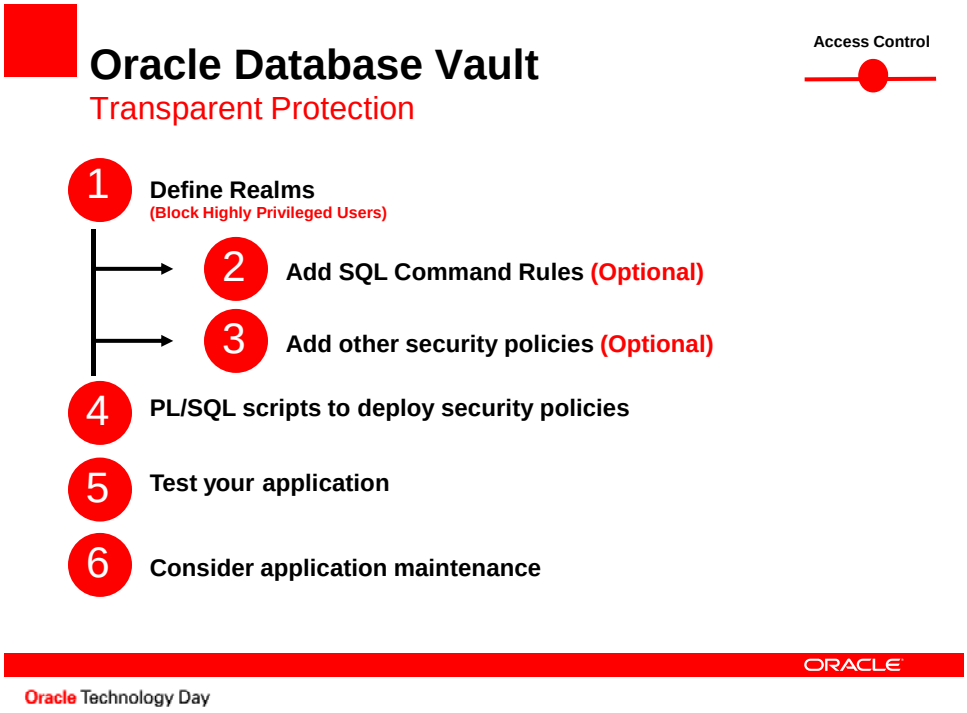
- Escaneo básico de configuraciones en 10g R1
- Mucho mejor en 10g R2 & superior.
- El siguiente release –manejo de configuraciones estándar.

Consideraciones para nuevos desarrollos

- No usar información tipo PII (personal Identifable Information) en llaves primarias o foráneas.
- Grabar tablas y vistas que contengan datos PII.
- Cumplimiento
- Auditoría
- Diseño de gestión de Usuarios con base en directorios.
- Aplicar el uso de tecnologías de esquema compartido.
- No usar “select user from dual” en “application code”

Diseño con nuevas tecnologías: Database Vault.

El flujo de tareas que se deben realizar para la protección de esquemas o base de datos con Oracle Database Vault son las siguientes:



Links de interés:

- Oracle Database Vault Best practices: http://www.oracle.com/technology/deploy/security/database-security/pdf/twp_database_vault_bestpractices_20080219.pdf
- Hands-On: http://www.oracle.com/technology/deploy/security/database-security/database-vault/index.html
- Preguntas y respuesta frecuentes: http://www.oracle.com/technology/deploy/security/database-security/database-vault/dbv_faq.html

ORACLE ADVANCED SECURITY OPTION

Qué es Oracle ASO?

Oracle Advanced Security es una opción de seguridad de la BD para Oracle Database 11g. Liberada desde la versión Oracle8i, Oracle Advanced Security combina capacidades de Cifrado en red, base de datos y autenticación fuerte todos juntos para ayudar a resolver los retos de las compañías en cuanto a requerimientos de privacidad cumplimiento:

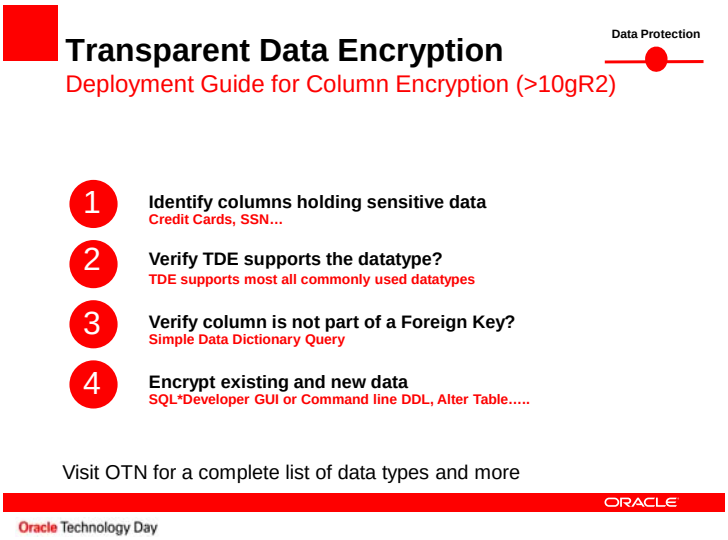
1. Cifrado transparente de datos TDE.
2. Cifrado de Red
3. Autenticación fuerte

TDE (Transparent Data Encryption)

TDE está diseñado para proveer a los clientes la habilidad de cifrar de manera transparente dentro de la base de datos sin impactar a las aplicaciones existentes. Retorna los datos en formato Cifrado podría impactar a las aplicaciones existentes. TDE provee la ventaja de Cifrar sin el impacto asociados a soluciones tradicionales de base de datos que típicamente requieren triggers y vistas. Oracle Database Vault puede ser usado para proteger los datos de las aplicaciones ante interacciones del DBA y otros usuarios privilegiados además de implementar robustos controles sobre el acceso a la base de datos y la aplicación.

TDE no soporta Cifrado de columnas con restricciones en llaves foráneas. Esto se debe al hecho de que cada tabla tiene su propia y única llave de Cifrado.

Los pasos para la configuración de Oracle TDE son los siguientes:



Identificar los datos sensitivos

Identificar información relacionada con datos PII (Personally Identifiable Information) tales como números de seguridad social y tarjetas de credito, se sugiere comenzar por una sencilla técnica en la que es fácil realizar búsquedas en el diccionario de datos de Oracle para encontrar nombres de columnas y tipos de datos que sean frecuentemente usados para almacenar esa 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 soporte de datos TDE

TDE soporta la mayoría de los tipos de datos más comunes usados en la base de datos, de los cuales se incluyen:

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

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

Cuando una columna indexada está para ser cifrada, se recomienda primero hacer drop de los índices existentes, cifrar la columna y finalmente reconstruir los índices.

Cambiar la llave de la Tabla/Columna

La llave de la tabla o la columna, el tamaño de la llave y el algoritmo pueden ser cambiados independientemente usando el comando alter table:

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

Cambiando la llave de la tabla o columna cifrará de nuevo todos los datos cifrados que se guardan en la tabla.

La lista de opciones de cifrado disponibles en Transparent Data Encryption son:

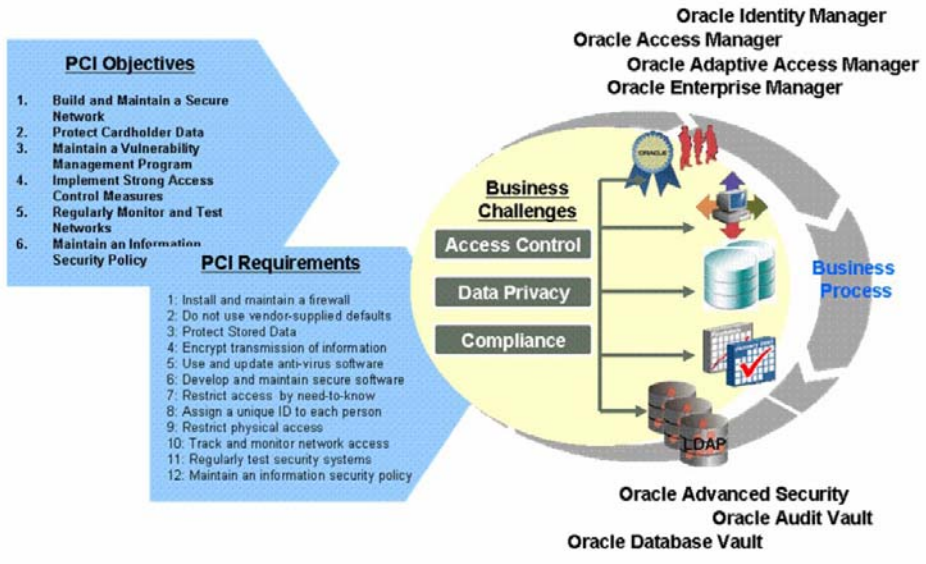
Package Feature	DBMS OBFUSCATION TOOLKIT (Oracle 8i and higher) SE & EE	DBMS CRYPTO (Oracle Database 10g R1 and higher) SE & EE	Oracle Advanced Security Transparent Data Encryption EE Only Option
Cryptographic algorithms	DES, 3DES	DES, DES, AES, RC4, 3DES_2KEY(1)	3DES, AES (128, 192, and 256 bit)
Padding forms	none supported	PKCS5, zeroes	PKCS5(2)
Block cipher chaining modes	CBC	CBC, CFB, ECB, OFB	CBC(2)
Cryptographic hash algorithms	MD5	SHA-1, MD4(1), MD5(1)	SHA-1(2)
Keyed hash (MAC) algorithms	none supported	HMAC_MD5, HMAC_SH1	n/a
Cryptographic pseudo-random number generator	RAW, VARCHAR2	RAW, NUMBER, BINARY_INTEGER	n/a
Database types	RAW, VARCHAR2	RAW, CLOB, BLOB	All but: OBJ., ADT, LOB

1) Provided for backward compatibility
2) Used Internally, not available to developers

Table 1. Oracle Database Encryption Overview

Cumplimiento de regulación PCI

Algunos de los controles proporcionados por Oracle Advanced Security Option resuelven requerimientos de la norma PCI (Payment Card Industry) que aunque no tiene aplicación por tipo de mercado al que pertenece Ecopetrol apoya la implantación de la definición de controles de seguridad.



Los controles que resuelve la solución Oracle Advanced Security Option son los siguientes:

- **Requerimiento 2**: No usar valores por defecto provistos por el proveedor y otros parámetros de seguridad. El Sub-requerimiento 2.1 trabaja con los parámetros por defecto establecidos por los proveedores y el sub-requerimiento 2.3 requiere cifrado de todos los accesos administrativos no-consola. En el ambiente, las cuentas del sistema tienen contraseñas por defecto? Qué tan fuerte son las contraseñas en las cuentas de Sistema? El acceso de los administradores requiere cifrado?.

  La respuesta de Oracle a este punto la resuelve la funcionalidad de cifrado provistas por Oracle Advanced Security tanto en al nivel de los datos en tránsito como en los residentes en la base de datos.

- **Requerimiento 3:** Proteger datos de tarjetabientes almacenados en la base de datos o que estén siendo transmitidos en la red. Con la funcionalidad de Transparent Data Encryption se provee cifrado de datos sensitivos en disco o en medios externos como cintas de manera transparente a las aplicaciones y usuarios; gestión automatizada de llaves, la aplicación no necesita modificaciones y los desarrolladores pueden focar su interés en la lógica de negocios sin requerir un entrenamiento profundo en temas de cifrado y gestión de llaves.

- **Requerimiento 4:** Encriptar las transmisiones de datos de los tarjetabientes a través de redes públicas.

Links de interés:

- Preguntas y respuestas frecuentes:
  http://www.oracle.com/technology/deploy/security/database-security/transparent-data-encryption/tde_faq.html

- Hands-On:
  http://www.oracle.com/technology/obe/10gr2_db_single/security/tde/tde_otn.htm

ORACLE DATAMASKING

Las organizaciones tienen la necesidad de compartir los datos de producción con los usuarios internos y externos para varios fines de negocio, como las pruebas de aplicación. Con Data Masking Pack, las organizaciones ahora pueden compartir la información interna de manera segura, y con los socios de negocio, y seguir cumpliendo con las regulaciones del gobierno. Los administradores de base de datos y seguridad de la información pueden mejorar su productividad al eliminar los procesos manuales y aplicar políticas de seguridad de la información a sus organizaciones.

Qué es?

Oracle Enterprise Manager Data Masking Pack brinda una solución completa y fácil de utilizar para compartir los datos de producción con las entidades internas y externas al tiempo que se evita que ciertas partes sensibles o confidenciales de la información sean reveladas a entidades no autorizadas

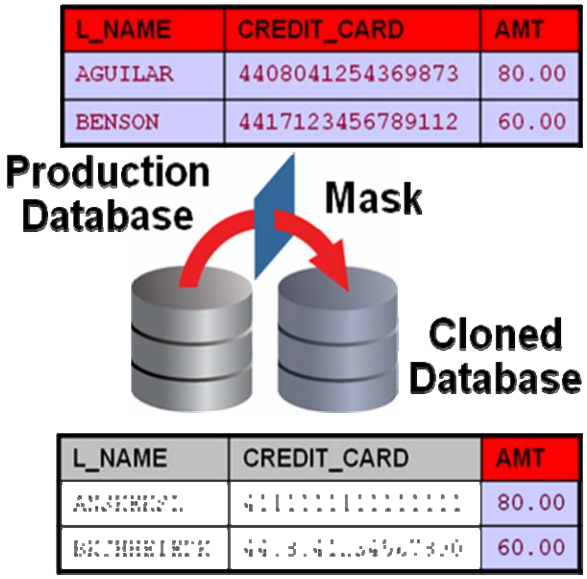
Data Masking y Cumplimiento Regulatorio

Resguardar los datos de producción y evitar la filtración de información confidencial o sensible a usuarios no productivos se ha vuelto un imperativo corporativo para todas las organizaciones– gracias al giro de regulaciones globales que gobiernan la privacidad de datos. La Ley Sarbanes Oxley de 2002 en los EE. UU. o la Ley de Instrumentos Financieros (FIEL) de Japón (también denominada J-SOX) brindan mejores estándares sobre los controles internos para la información corporativa. La Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA) de 1996 en los EE. UU. o la Directiva sobre la Protección de Datos en la Unión Europea son parte de las leyes globales que rigen la privacidad de los datos personales relacionados con los individuos. Incluso los procesadores de pagos con tarjeta de crédito han adoptado los estándares de la Industria de Tarjetas de Pago (PCI) respecto del uso y la distribución de información sobre tarjetas de crédito.

Las organizaciones siempre han mantenido la información confidencial, personalmente identificable o sensible en sus bases de datos de producción. Estas organizaciones deben proteger el uso y la distribución de la información en cumplimiento con las regulaciones, o arriesgarse a las multas y penalidades que implica la violación a estas leyes sobre privacidad de datos. Estas multas y penalidades pueden ser de miles de dólares por día. En consecuencia, ninguna organización puede permitirse violar estas leyes y arriesgar la indigna publicidad causada por violaciones no autorizadas a los datos.

Data Masking Pack puede ayudar a las organizaciones a cumplir con las leyes de privacidad y confidencialidad al enmascarar los datos sensibles o confidenciales en los entornos de desarrollo, prueba o staging. Data Masking Pack utiliza un proceso irreversible para reemplazar los datos

sensibles con datos que parecen reales pero que están cancelados sobre la base de reglas de enmascaramiento, y garantiza que los datos originales no puedan ser recuperados ni restaurados. Data Masking Pack ayuda a mantener la integridad de la aplicación mientras enmascara los datos.



Formatos de Enmascaramiento

Las organizaciones tienen la información sensible, confidencial o personalmente identificable almacenada en varias columnas dentro de las tablas de base de datos. Estos grupos de información son bastante diferentes y son candidatos al enmascaramiento de datos. En la actualidad, este es un problema central para las organizaciones porque los DBA a menudo eligen implementar soluciones distintas basadas en scripts para el enmascaramiento de datos en cada base de datos. Al tener una definición central para formatos de enmascaramiento común en Data Masking Pack, las empresas pueden aplicar las reglas para privacidad de datos consistentemente en todos los datos de producción y, en consecuencia, garantizar el cumplimiento de las regulaciones. Data Masking Pack puede alojar una gran variedad de datos mediante el uso de formatos de enmascaramiento.

Data Masking Pack brinda elementos básicos de enmascaramiento listos para usar para varios tipos de datos, como números aleatorios, dígitos aleatorios, fechas aleatorias, constantes. Las organizaciones también pueden utilizar otras rutinas de enmascaramiento, como el cambio, que cambia el valor de una columna a lo largo de varias filas. Esto es útil cuando el rango de valores de una columna no se conoce y el cambio de valores en la misma tabla ofrece un grado suficiente de protección a la privacidad. Para las organizaciones que requieren que el valor enmascarado sea realista pero no esté basado en los datos originales, Data Masking Pack puede reemplazar los

datos originales, como nombres y direcciones, por datos que contienen nombres y direcciones ficticias provenientes de fuentes de datos externas.

Format Library

The Format Library contains a collection of ready-to-use masking formats which can be used when creating a masking definition.

Search Format Go Export Import Create

View Create Like Edit Delete

Select	Format	Data Type	Sample	Description	Owner
◉	Constant value (in Simplified Chinese)	Character	格式名称	格式说明	SYSMAN
○	Anglo-American Last Names	Source Type	Adjani	Realistic but fictitious last names of US or UK origin	SYSMAN
○	US National Identifiers (SSN)	Character	111-39-9600	Random social security numbers for US employees	SYSMAN
○	Bay Area phone numbers	Character	(415) 555-0100	Dummy phone numbers based on area codes in the Bay Area	SYSMAN
○	Visa or Mastercard Credit Card Numbers	Character	5932521262645000	PCI-compliant dummy credit card numbers with checksum	SYSMAN

Una organización con requisitos de enmascaramiento especializado también puede agregar formatos de enmascaramiento definidos por usuarios al grupo de formatos de enmascaramiento. Estos formatos definidos por usuarios, que están definidos mediante PL/SQL, ofrecen un grado ilimitado de flexibilidad al generar el formato de enmascaramiento adecuado para la empresa o el segmento de la industria en el que opera la organización. Los administradores de seguridad de la información pueden luego crear máscaras complejas y compuestas de acuerdo con combinaciones de varios formatos de enmascaramiento – tanto estándar como definidas por usuarios. Por ejemplo, una máscara para números comunes de tarjetas de crédito puede estar definida por exclusivos números de dieciséis dígitos que comienzan con 4 ó 5, que luego son verificados para que las sumas de verificación sean compatibles con los estándares PCI.

Como buena práctica corporativa, es recomendable que las organizaciones definan los formatos de enmascaramiento estándar para la información sensible comúnmente enmascarada, como identificadores nacionales o números de seguridad social, números de tarjetas de crédito, etc. para garantizar la aplicación uniforme de los procesos de protección de la privacidad de datos.

Definición de Enmascaramiento

Las actuales aplicaciones empresariales tienen esquemas de base de datos muy complejos que contienen cientos o miles de objetos de base de datos. Los administradores tienen la desalentadora tarea, que a su vez consume mucho tiempo, de identificar todas las tablas y columnas que contienen información confidencial o sensible, y organizarlas en los formatos adecuados de enmascaramiento. Afortunadamente, Data Masking Pack facilita esta tarea mediante la función de búsqueda incorporada que permite que el administrador de seguridad de la información consulte todo el diccionario de datos a fin de identificar las columnas o tablas potenciales que contienen los datos sensibles.

Masking Definition: Employee mask

A data masking definition specifies what columns to be masked and the format of masked data.

Name **Employee mask** Database **Human Resources** Description

Columns

Owner	Table Name	Column Name	Format
HR	EMPLOYEES	EMPLOYEE_ID	

Foreign Key Columns

Owner	Table Name	Column Name	Parent Owner	Parent Table	Parent Column
HR	DEPARTMENTS	MANAGER_ID	HR	EMPLOYEES	EMPLOYEE_ID
HR	EMPLOYEES	MANAGER_ID	HR	EMPLOYEES	EMPLOYEE_ID
HR	JOB_HISTORY	EMPLOYEE_ID	HR	EMPLOYEES	EMPLOYEE_ID
OE	CUSTOMERS	ACCOUNT_MGR_ID	HR	EMPLOYEES	EMPLOYEE_ID
OE	ORDERS	SALES_REP_ID	HR	EMPLOYEES	EMPLOYEE_ID

Dependent Columns

Owner	Table Name	Column Name	Parent Owner	Parent Table	Parent Column
HR	MANAGERS	MGR_ID	HR	EMPLOYEES	EMPLOYEE_ID

Una vez seleccionada una columna para el enmascaramiento, Data Masking Pack automáticamente identifica todas las columnas relacionadas con las columnas y las tablas seleccionadas de acuerdo con las relaciones de integridad referencial de clave externa mantenidas en el diccionario de datos. Esto asegura que la regla de enmascaramiento aplicada a la columna primaria también se aplique automáticamente a otras tablas y columnas asociadas. En determinadas circunstancias, cuando la integridad referencial de los datos se mantiene en la lógica de aplicaciones en lugar de en la base de datos, Data Masking Pack permite que los administradores de base de datos agreguen las tablas y columnas asociadas mediante la capacidad

Related Application Column (Columna de Aplicación Relacionada). Esto garantiza que los datos de aplicaciones sigan siendo consistentes independientemente de si la integridad referencial de la aplicación se mantiene en la base de datos o en otro lugar.

Una vez que la definición de enmascaramiento o el mapeo de tablas y columnas a formatos de enmascaramiento está completo, los administradores o desarrolladores de aplicaciones pueden guardar esta definición en un formato XML portable denominado Plantilla para Enmascaramiento de Aplicaciones utilizando la capacidad Exportar Definición de Enmascaramiento. Esto permite que los administradores restauren la definición de enmascaramiento incluso si la definición original ha sido alterada. En los casos donde hay distintas instalaciones de Enterprise Manager Grid Control que administran las bases de datos con esquemas similares de aplicaciones, los administradores pueden importar estas definiciones de enmascaramiento con rapidez y pueden estar preparados para enmascarar los datos. Al estar los formatos de enmascaramiento definidos y las definiciones de enmascaramiento completas, el administrador empresarial ahora está listo para proceder con el proceso de enmascaramiento.

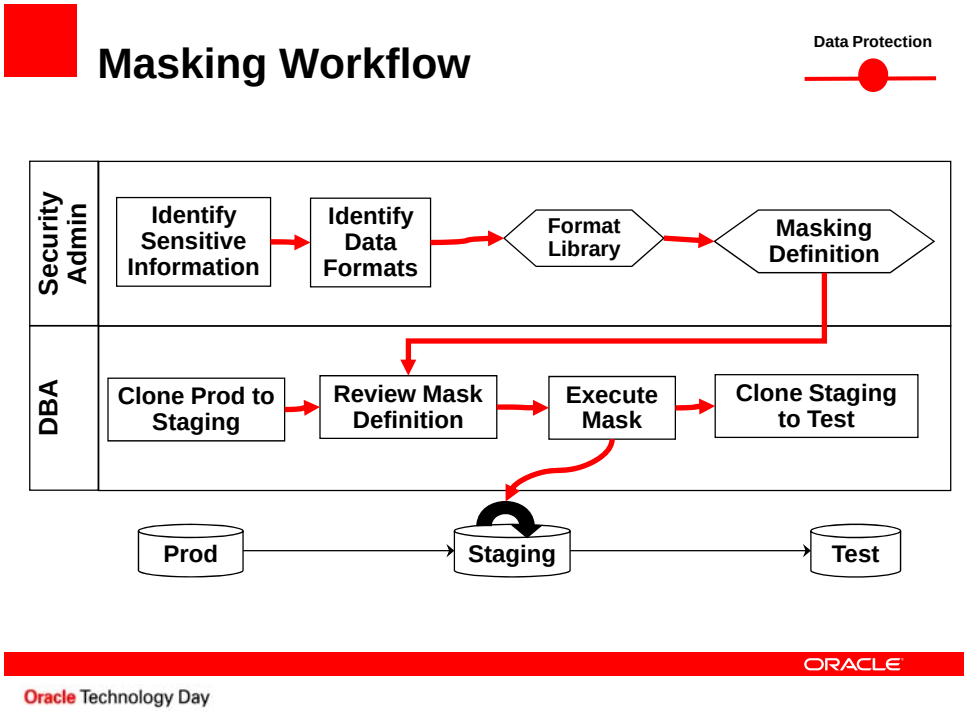
Proceso de Enmascaramiento

Antes de iniciar el proceso de enmascaramiento, Data Masking Pack realiza una serie de pasos de validación para garantizar que el proceso de enmascaramiento de datos prosiga hacia un fin exitoso sin errores. Algunas de las verificaciones que realiza incluyen validar los formatos de enmascaramiento. Este es un paso necesario en el proceso de enmascaramiento de datos para garantizar que los formatos de enmascaramiento elegidos cumplan con los requerimientos de integridad de las aplicaciones y la base de datos. Estos requerimientos pueden incluir la generación de valores exclusivos de la columna que se enmascara debido a restricciones de exclusividad o la generación de valores que cumplen con los requisitos de tipo y longitud de columna.

Data Masking Pack utiliza un mecanismo altamente eficiente y sólido para crear datos enmascarados. Data Masking realiza operaciones en bloque para reemplazar con rapidez la tabla que contiene datos sensibles por una tabla idéntica que contiene datos enmascarados, y reteniendo al mismo tiempo las restricciones de la base de datos original, estructuras asociadas de acceso e integridad referencial, como ÍNDICES, PARTICIONES y permisos de acceso, como GRANTs. A diferencia de los procesos de enmascaramiento que son tradicionalmente lentos debido a que realizan actualizaciones de tabla, Data Masking Pack aprovecha las optimizaciones incorporadas en la base de datos para desactivar el ingreso a la base de datos y lograr una ejecución en paralelo para crear rápidamente un reemplazo enmascarado de la tabla original. La tabla original que contiene datos sensibles se elimina completamente de la base de datos y ya no es accesible.

Los administradores de base de datos cuentan con la flexibilidad de programar el proceso de enmascaramiento en una ventana adecuada para el mantenimiento, de manera que el proceso de enmascaramiento puede iniciarse justo después de que se haya clonado la base de datos de producción en un entorno staging. Para los DBA avanzados, Data Masking Pack proporciona la opción de guardar el proceso de enmascaramiento como un script de manera que se pueda personalizar más adelante, de acuerdo con las necesidades de su organización.

A continuación se resume el flujo de actividades asociadas al enmascaramiento de los datos usando Oracle DataMasking.



Links de interés:

- Información general del Paquete Data Masking: http://www.oracle.com/enterprise_manager/data-masking.html
- Hands-On: http://www.oracle.com/technology/obe/11gr1_db/security/datamask/datamask.htm