Oracle Database 11g Versión 1
Soluciones Transparentes para la Seguridad y el Cumplimiento

Informe Ejecutivo de Oracle

Junio de 2007

ORACLE

INTRODUCCIÓN

Durante los últimos diez años, han surgido varias regulaciones que imponen estrictos controles internos y la protección de información personalmente identificable (PII). Algunos ejemplos de dichas regulaciones incluyen Sarbanes-Oxley (SOX), PCI, HIPAA, Ley de Intercambio e Instrumentos Financieros, Basilea II y la Directiva de la UE sobre Privacidad y Comunicaciones Electrónicas en Europa. El continuo surgimiento de nuevas regulaciones en todo el mundo junto con la naturaleza cada vez más sofisticada del robo de información requiere una estricta seguridad de datos.

AMÉRICA
- **Sarbanes-Oxley (SOX)**
- **Ley de Transferencia y Responsabilidad de Seguros Médicos (HIPAA)**
- **CA SB 1386 y otras Leyes Federales de Privacidad**
- **Ley de Seguridad de Datos de la Industria de Tarjetas de Pago**
- **FDA CFR 21 Sección 11**
- **FISMA (Ley Federal de Administración de Seguridad de la Información)**

EMEA
- **Directivas de Privacidad de la UE**
- **Ley de Sociedades del Reino Unido de 2006**

APAC
- **Ley de Intercambio e Instrumentos Financieros (J-SOX)**
- **CLERP 9: Ley de Privacidad Corporativa y Reforma de Auditorías (Australia)**

GLOBAL
- **Estándares Internacionales de Contabilidad**
- **Basilea II (Banca Global)**
- **Pautas OECD sobre Gobierno Corporativo**

Figura 1. Desafíos de Privacidad y Cumplimiento

Los estudios sobre Seguridad y Delitos Informáticos de CSI/FBI 2005 han documentado que más del 70% de los ataques y la pérdida de datos de los sistemas de información han sido cometidos por integrantes de la organización, es decir, por aquellas personas por lo menos con autorización en algún nivel de acceso al sistema y sus datos. Las soluciones transparentes de seguridad son críticas en la actual economía global de negocios. Oracle Database 11g versión 1 brinda las capacidades más avanzadas del sector respecto de la seguridad de los datos, con soluciones de seguridad que funcionan de manera transparente con las aplicaciones existentes, mientras se cumple con los requerimientos obligatorios de las regulaciones.

SOLUCIONES TRANSPARENTES DE SEGURIDAD

Las soluciones transparentes de seguridad son críticas porque históricamente la mayoría de las aplicaciones ha dependido de la seguridad en el nivel de aplicaciones para restringir el acceso a los datos sensibles. Los conceptos de seguridad como *privilegio mínimo* y *necesidad de conocimiento* fueron considerados menos importantes que la escalabilidad y la rápida implementación de nuevas aplicaciones. Internet aceleró el desarrollo de nuevas aplicaciones para todos los aspectos del procesamiento de negocios, dando como resultado una mejor accesibilidad, grandes ahorros de costo y aumentos de productividad. No obstante, las regulaciones mundiales ahora

requieren controles más estrictos sobre información financiera sensible y relacionada con la privacidad. Los productos de Oracle Database Security simplifican la transición de la seguridad en el nivel de aplicaciones a la seguridad activada por la base de datos, permitiendo que las organizaciones minimicen los costos relacionados con el cumplimiento regulatorio y la implementación de estrictos controles internos. Oracle Database Security brinda soluciones transparentes para la seguridad de aplicaciones en las áreas críticas de administración de usuarios, control de acceso, protección de datos y monitoreo.

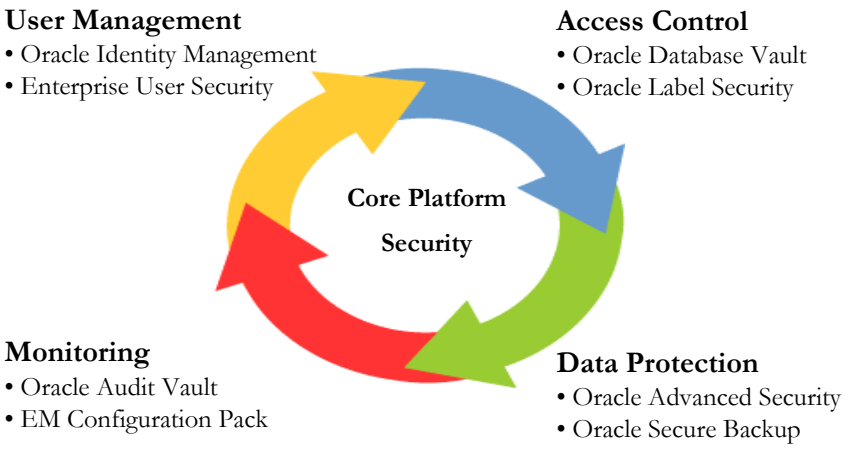

Figura 2. Productos de Oracle Data Security

ORACLE DATABASE 11G VERSIÓN 1 ADMINISTRACIÓN DE USUARIOS

La provisión eficiente y la no provisión de usuarios de base de datos constituyen una parte importante de la arquitectura de seguridad empresarial. La seguridad de usuarios empresariales de Oracle Database permite que los administradores administren a los usuarios de base de datos en Oracle Identity Management o su directorio corporativo utilizando Oracle Virtual Directory.

Seguridad de Usuarios Empresariales

La seguridad de usuarios empresariales permite que miles de usuarios sean administrados centralmente en un directorio corporativo existente. Los usuarios pueden autenticarse individualmente utilizando una contraseña, Kerberos o credencial PKI y compartir una sola cuenta de la base de datos, simplificando así la administración de usuarios y aumentando la seguridad. Por ejemplo, una sola cuenta de la base de datos denominada '*Org A*' podría definirse en la base de datos Oracle, y los usuarios de la *Unidad de Negocios A* podrían asignarse a la nueva cuenta. La necesidad de cuentas individuales en la base de datos se ve reducida. Se pueden crear roles globales para SYSDBA y SYSOPER en Oracle Identity Management, lo cual es nuevo en Oracle Database 11g versión 1. Las organizaciones con grandes cantidades de bases de datos pueden administrar centralmente el acceso SYSDBA y SYSOPER a varias bases de datos empresariales. La capacidad de administración para seguridad de usuarios empresariales ha sido integrada con Enterprise Manager Database Control, algo nuevo en Oracle Database 11g versión 1. Asimismo, Oracle recientemente completó las pruebas de seguridad de usuarios empresariales con Oracle Virtual Directory. Oracle Virtual Directory permite que la seguridad de usuarios empresariales de Oracle Database trabaje con directorios corporativos existentes como Microsoft Active Directory, simplificando drásticamente la administración de usuarios de la base de datos Oracle.

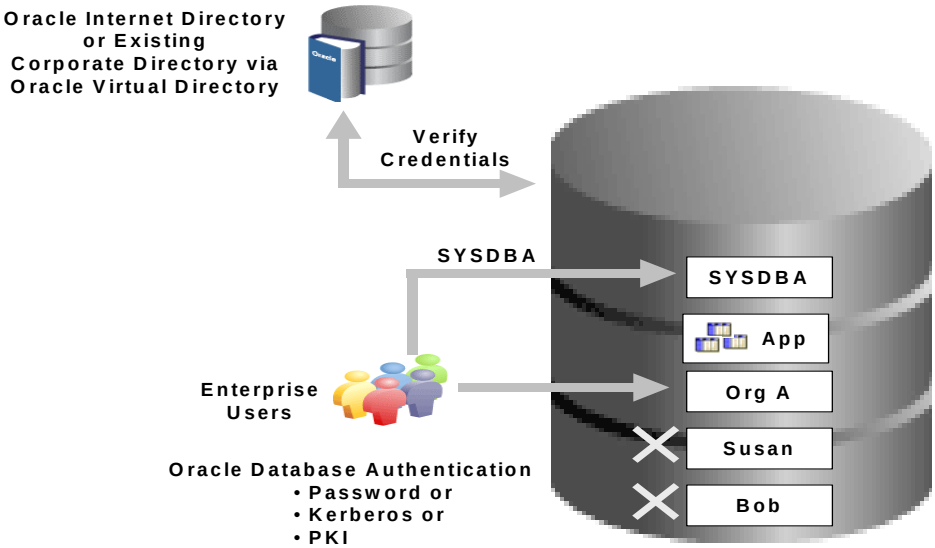

Figura 3. Oracle Database Enterprise User Security con Oracle Identity Management

ORACLE DATABASE 11G VERSIÓN 1 CONTROL DE ACCESO

La Base de Datos Oracle ofrece los controles de acceso más avanzados de la industria. Durante los últimos 30 años, Oracle ha incorporado poderosas características para el control de acceso como Virtual Private Database y Oracle Label Security. Cumplir con los estrictos requerimientos de control interno de las regulaciones requiere el control de acceso a bases de datos, aplicaciones y datos desde el interior de la base de datos y la reducción de obligaciones en el nivel de aplicaciones.

Oracle Database Vault

Oracle Database Vault es la solución de seguridad líder más reciente del sector de Oracle diseñada específicamente para proteger los datos de negocio para el cumplimiento regulatorio y reducir el riesgo asociado con las amenazas internas. Ya sea que se trate de aplicaciones cliente servidor tradicionales o de aplicaciones basadas en la Web, Oracle Database Vault brinda controles de seguridad flexibles, transparentes y altamente adaptables sin la necesidad de realizar cambios en las aplicaciones. Oracle Database Vault recientemente obtuvo el premio 2007 a la Excelencia Global en Seguridad de Base de Datos, otorgado por Info Security Products Guide. Oracle Database Vault está disponible para Oracle Database 9i versión 2, Oracle Database 10g versión 2 y Oracle Database 11g versión 1. Además, Oracle Database Vault ha sido validado con las Aplicaciones Oracle PeopleSoft. Actualmente, se encuentra en proceso la validación con otras aplicaciones, como Oracle E-Business Suite y Siebel.

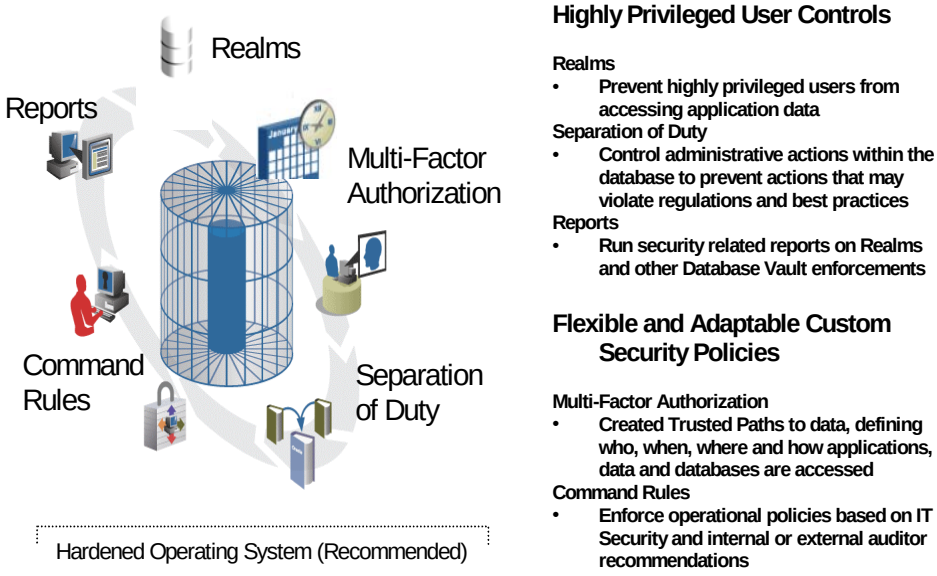

Figura 4. Generalidades sobre Oracle Database Vault

Oracle Database Vault Realms

Oracle Database Vault Realms evita que los DBA, propietarios de aplicaciones y otros usuarios privilegiados vean los datos de aplicaciones utilizando sus poderosos privilegios. Oracle Database Vault Realms pone en marcha controles preventivos, ayudando a reducir el impacto potencial cuando se produce una violación a los datos, permitiendo que el DBA realice su trabajo con más eficiencia. Oracle Database Vault Realms puede utilizarse para proteger toda una aplicación o un grupo específico de tablas dentro de una aplicación, ofreciendo exigencias de seguridad altamente flexibles y adaptables.

Oracle Database Vault – Separación de Tareas

La separación de tareas de Oracle Database Vault permite realizar un enfoque sistemático hacia la seguridad, lo cual fortalece los controles internos dentro de la base de datos. Oracle Database Vault crea tres responsabilidades distintas dentro de la base de datos.

- Administración de cuentas
- Administración de seguridad
- Administración de recursos

Responsabilidad	Descripción
Administración de Cuentas	Un usuario con la responsabilidad de administración de cuentas puede crear, dar de baja o modificar usuarios de la base de datos. Se evitará que los usuarios existentes con altos privilegios realicen actividades de administración de cuentas.
Administración de Seguridad	La responsabilidad de administración de seguridad está diseñada para permitir que un usuario se convierta en administrador de seguridad (Propietario de Database Vault) de la base de datos. Un administrador de seguridad puede establecer Database Vault Realms, Reglas de Comando, autorizar a otros usuarios a utilizarlos y realizar varios informes de seguridad específicos de Database Vault. Se evita que el administrador de seguridad autorice por sus propios medios el acceso a los datos de negocio seguros.
Administración de Recursos	La responsabilidad de administración de recursos permite que un usuario con los privilegios de DBA siga realizando el mantenimiento y la administración normal asociada con la base de datos, como backup y recuperación, parches y ajuste de desempeño.

Tabla 2. Oracle Database Vault – Separación de Tareas

La extensibilidad de Oracle Database Vault permite que la separación de tareas se personalice de acuerdo con sus requerimientos específicos de negocio. Por ejemplo, usted puede subdividir aún más la responsabilidad de administración de recursos en responsabilidades de backup, desempeño y parches. Si se trata de una empresa pequeña, puede consolidar las responsabilidades o asignar diferentes cuentas de ingreso para cada responsabilidad, permitiendo una auditoría y responsabilidad más granular.

Oracle Database Vault brinda numerosos informes listos para usar que otorgan la capacidad de informar por ejemplo sobre el intento de acceso a datos bloqueado por Realms. Por ejemplo, si un DBA intenta acceder a los datos desde una tabla de aplicaciones protegida por Realm, Database Vault creará un registro de auditoría en una tabla especialmente protegida dentro de Database Vault. Oracle Database Vault incluye un informe de violación Realm que facilita la visualización de estos registros de auditoría.

Controles Flexibles y Extensibles de Acceso

La proliferación de regulaciones y leyes de privacidad alrededor del mundo requiere políticas de seguridad flexibles y altamente adaptables que puedan ser fácilmente modificadas para cumplir con los requerimientos existentes y recientemente emergentes de los controles de acceso. Para complicar aún más los requerimientos del control de acceso existen problemas como aplicaciones *out-sourcing* y *hosted* o a pedido. Oracle Database Vault presenta capacidades avanzadas exclusivamente adecuadas para cumplir con éstos y futuros requerimientos de control de acceso.

Oracle Database Vault - Autorización de Factores Múltiples

La Autorización de Factores Múltiples de Oracle Database Vault extiende los controles de acceso más allá del control de acceso tradicional basado en roles y del control incluso más sofisticado basado en etiquetas que se encuentra en la Base de Datos Oracle. Al utilizar la autorización de factores múltiples, el acceso a las bases de datos puede ser restringido a una subred o servidor de aplicaciones, creando un

proceso confiable virtual para el acceso a datos. Limitar el acceso a datos a las aplicaciones aprobadas puede lograrse utilizando factores Oracle Database Vault junto con las Reglas de Comando de Oracle Database Vault. Oracle Database Vault ofrece algunos Factores incorporados, como la dirección de IP, que pueden utilizarse individualmente o juntos en combinación con otras reglas de seguridad a fin de elevar significativamente el nivel de seguridad para una aplicación existente. Además de los Factores incorporados ofrecidos por Oracle Database Vault, usted puede agregar sus propios factores personalizados para cumplir con los requerimientos de negocio.

Reglas de Comando de Oracle Database Vault

Las Reglas de Comando de Oracle Database Vault ofrecen la capacidad de agregar fácilmente políticas de seguridad a casi cualquier operación de base de datos. Las Reglas de comando permiten fortalecer los controles internos, imponer las mejores prácticas del sector y asegurar las políticas de configuración. Las Reglas de Comando pueden utilizarse para imponer una protección estricta sobre datos de negocio críticos. Por ejemplo, una regla de comando puede utilizarse para evitar que cualquier usuario, incluso el DBA, elimine tablas de aplicaciones en su entorno de producción. Las Reglas de Comando pueden administrarse fácilmente mediante la consola de Oracle Database Vault o en la línea de comando utilizando la API.

Oracle Label Security

Oracle Label Security permite el control transparente de acceso en el nivel de filas de la base de datos Oracle utilizando etiquetas de sensibilidad. Utilizadas junto con Oracle Database Vault, las etiquetas de sensibilidad se vuelven factores poderosos para utilizar en el proceso de autorización de factores múltiples, lo cual ayuda a cumplir con los requerimientos de cumplimiento regulatorio. Altamente flexible y adaptable, Oracle Label Security es el producto más avanzado del sector para el control de acceso basado en etiquetas. La administración basada en políticas simplifica la administración de etiquetas de sensibilidad y autorizaciones de etiquetas de usuarios.

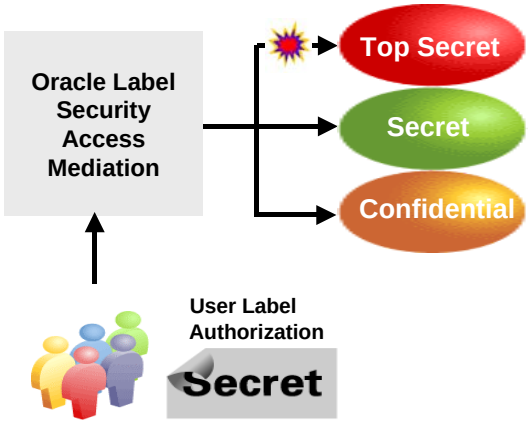

Figura 5. Generalidades sobre Oracle Label Security

Proteger los Datos Sensibles
Oracle Label Security controla transparentemente el acceso a los datos de aplicaciones al comparar las etiquetas de sensibilidad de datos con las autorizaciones de etiquetas. Al utilizar Oracle Enterprise Manager, los administradores de seguridad pueden definir las etiquetas de sensibilidad de datos y asignar autorizaciones de etiquetas a los usuarios, con inclusión de la etiqueta de sensibilidad máxima a la que un usuario individual está autorizado a acceder. Los administradores de seguridad pueden luego aplicar políticas Label Security a una o más tablas de aplicaciones. Una vez aplicadas, Label Security mediará transparentemente el acceso a los datos de aplicaciones al comparar las autorizaciones de etiqueta de los usuarios con la etiqueta de sensibilidad asignada a los datos. Solo si la autorización de etiqueta del usuario es igual o mayor que el nivel de sensibilidad de los datos, se otorgará el acceso a los datos. Las etiquetas de sensibilidad de datos pueden incluir tres componentes.

• Nivel obligatorio, jerárquico *más*

• Ninguna subdivisión o más divisiones horizontales *más*

• Ningún grupo o más grupos *parent child* (principal-secundario).

Por ejemplo, la etiqueta de sensibilidad *Secret*: *ProjectAthens:ExecOnly* está compuesta por el nivel *Secret*, la subdivisión *ProjectAthens* y el grupo *ExecOnly*. Muchas organizaciones pueden elegir solo utilizar el componente de nivel.

Integrado con Oracle Database Vault
Utilizadas junto con Oracle Database Vault, las etiquetas de sensibilidad se vuelven factores poderosos para su uso en autorizaciones de factores múltiples, ayudando a cumplir con los requisitos de cumplimiento regulatorio. Por ejemplo, las autorizaciones de etiquetas de usuarios pueden utilizarse en las reglas de comando de Oracle Database Vault para controlar el acceso a la base de datos, los comandos SQL y las tablas de aplicaciones. Esta ponderosa capacidad nueva extiende los conceptos de Label Security más allá de los controles tradicionales del acceso en el nivel de filas hacia la mediación en el nivel de base de datos y aplicaciones. La separación de tareas de Oracle Database Vault puede extenderse. Por ejemplo, las actividades de administración de base de datos podrían basarse en la autorización de etiquetas del administrador.

Flexible y Adaptable
Oracle Label Security ofrece múltiples opciones de ejecución para el control de acceso en el nivel de filas. Se pueden aplicar políticas solo para operaciones de lectura, actualizar las operaciones solamente, o ambas. Las autorizaciones de etiquetas de usuarios incluyen una etiqueta de lectura máxima, etiqueta de escritura por defecto y etiqueta de sesión por defecto. La etiqueta de lectura máxima especifica la etiqueta de sensibilidad de datos máxima a la que un usuario está autorizado a acceder, la etiqueta de escritura por defecto es la etiqueta de sensibilidad de datos por defecto asignada a los datos que ingresa el usuario, y la etiqueta de sesión por defecto es la etiqueta de sensibilidad por defecto que tiene un usuario cuando se conecta a la base de datos. Esto debe ser igual o menor a la etiqueta de lectura máxima. A los usuarios y procedimientos almacenados se les puede otorgar autorizaciones especiales que permiten el acceso a todos los datos para realizar operaciones de lectura o actualización independientemente de las autorizaciones de etiquetas de usuarios. Las autorizaciones especiales son útiles para fines de mantenimiento y creación de parches. La capacidad proxy para el único modelo de aplicaciones de usuarios es suministrada mediante la autorización de acceso a perfiles Label Security, permitiendo que el usuario primario de aplicaciones se haga cargo de las autorizaciones de etiquetas de un usuario de aplicaciones. Las cláusulas ‘where’ o predicados SQL pueden incorporarse opcionalmente en cualquier política Label Security, extendiendo el control de acceso más allá de la etiqueta de sensibilidad. Tenga en cuenta que las autorizaciones de etiquetas pueden ser asignadas a los usuarios de aplicaciones.

Capacidad de Administración Simplificada
Oracle Label Security ofrece un modelo de administración basado en políticas y fácil de utilizar. Las políticas son los contenedores lógicos de las etiquetas de sensibilidad, autorizaciones de etiquetas y, de manera opcional, los objetos protegidos. Puede haber varias políticas en la misma base de datos. La integración opcional con Oracle Identity Management brinda una administración centralizada de las políticas y las autorizaciones de etiquetas de usuarios. Además de la consola Enterprise Manager Label Security, se ofrece una API Label Security completa.

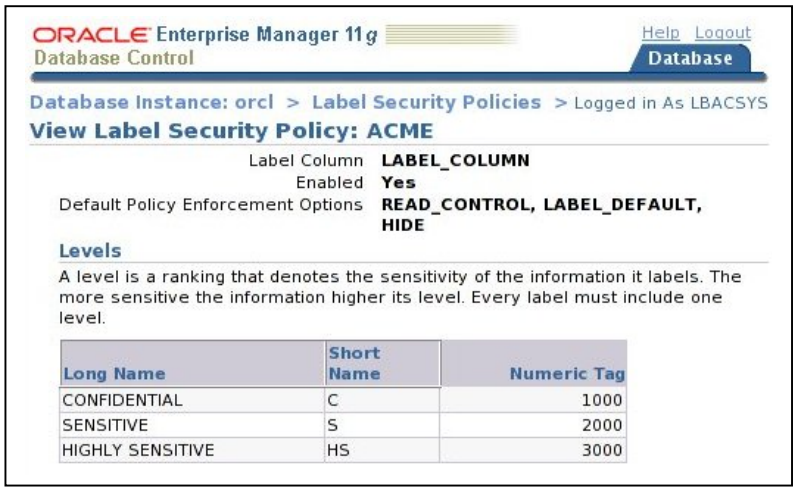

Figura 6. Capacidad de Administración de Oracle Label Security

ORACLE DATABASE 11G VERSIÓN 1 – PROTECCIÓN DE DATOS

La encriptación es una de las tecnologías de seguridad más antiguas del mercado. Sin embargo, durante los últimos 5 años, la necesidad de encriptación ha aumentado debido a problemas como el robo de identidad y la pérdida de medios. El robo de números de seguridad social, números de tarjetas de crédito y propiedad intelectual es un problema grave, y la necesidad de proteger la información relacionada con la privacidad va desde la educación superior hasta el sector minorista y casi cualquier negocio alrededor del mundo. La base de datos Oracle ofrece la mejor protección de la industria en cuanto a datos incluidos en la base de datos. Una vez que los datos son eliminados de la base de datos y pasan al disco, la cinta o la red, la única solución es la encriptación.

Oracle Advanced Security

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

Encriptación Transparente de Datos

La encriptación transparente de datos (TDE) de Oracle Advanced Security brinda encriptación sólida para resguardar los datos sensibles contra el acceso no autorizado en el nivel del sistema operativo o 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 los números de seguridad social y los números de tarjetas de crédito. Con un comando *alter table* simple, 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 para encriptación de base de datos, TDE es completamente transparente para las aplicaciones existentes, sin *triggers*, visualizaciones ni cambios en las aplicaciones. Los datos se encriptan en forma transparente cuando se escriben en el disco, y se decodifican en forma transparente después de que un usuario de aplicaciones ha autenticado y aprobado con éxito todos los controles de autorización. Los controles de autorización incluyen la verificación de que el usuario tiene los privilegios *select* y *update* (seleccionar y actualizar) necesarios en la tabla de aplicación, y la verificación de las políticas de

Database Vault, Label Security y Virtual Private Database. Las rutinas de backup de la base de datos seguirán funcionando, y los datos permanecerán encriptados en el backup. Para la encriptación de backups de toda la base de datos, TDE puede utilizarse junto con Oracle RMAN.

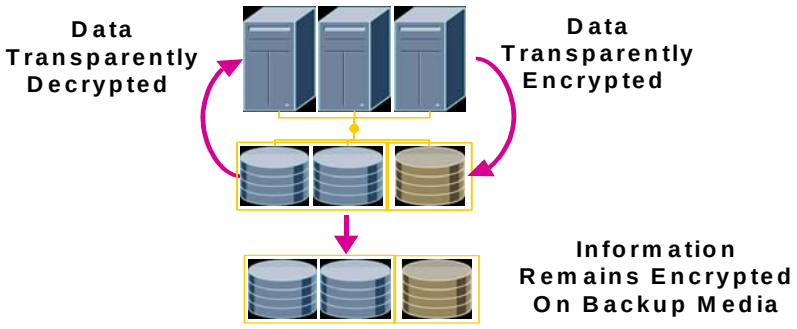

Figura 7 Generalidades sobre la Encriptación Transparente de Datos

Encriptación del Espacio de Tabla

Oracle Advanced Security en Oracle Database 11g versión 1 incluye soporte de encriptación del espacio de tabla. Cuando se crea un espacio de tabla mediante Enterprise Manager o en la línea de comando, hay 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 datapump, se encriptarán tablas enteras de manera transparente. Cuando la base de datos lee los bloques de datos del espacio de tabla encriptado, decodificará transparentemente los bloques de datos.

Módulos de Seguridad de Hardware

TDE ha sido mejorado en Oracle Database 11g versión 1 para respaldar el almacenamiento de la clave de encriptación TDE maestra externamente en un dispositivo de módulo de seguridad de hardware (HSM). Esto brinda 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.

Sólida Protección para Datos en Tránsito

Oracle Advanced Security brinda una solución integral, fácil de implementar, para proteger todas las comunicaciones desde y hacia la base de datos Oracle, ofreciendo encriptación de red nativa y basada en SSL. La autenticación y encriptación basada en SSL está disponible para empresas que han implementado Public Key Infrastructure (Infraestructura de Clave Pública). El soporte para el protocolo TLS 1.0 (incluidas las suites de códigos AES) fue introducido con Oracle Database 10g versión 1. Oracle Database puede configurarse para rechazar conexiones de clientes sin encriptación o permitir, opcionalmente, las conexiones no encriptadas para la flexibilidad de implementación. La configuración de 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.

ORACLE DATABASE 11G VERSIÓN 1 - MONITOREO

La base de datos Oracle proporciona capacidades de auditoría, tanto estándar con detallada. La auditoría nunca ha sido más importante que ahora. Se ha vuelto un recurso de seguridad clave para ayudar a acelerar los informes de cumplimiento regulatorio y detectar proactivamente la actividad sospechosa. La naturaleza cada vez más sofisticada de amenazas de seguridad requiere un enfoque minucioso de defensa hacia la seguridad que incluye el monitoreo integral de su empresa.

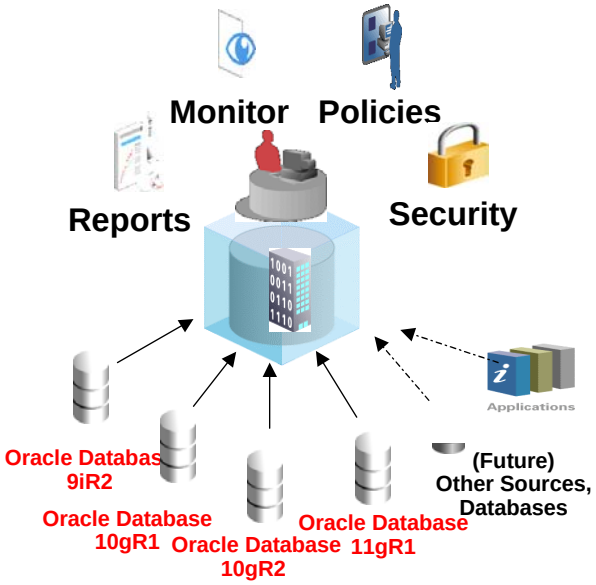

Figura 8. Generalidades sobre Oracle Audit Vault

Oracle Audit Vault

Oracle Audit Vault reduce el costo y la complejidad de cumplimiento y el riesgo de amenazas internas al automatizar la recopilación y consolidación de datos de auditoría. Brinda un depósito de auditoría seguro y altamente escalable, lo cual permite la realización de informes simplificados, análisis y una detección más simple de amenazas respecto de los datos de auditoría. Asimismo, los parámetros de auditoría de base de datos se administran y monitorean centralmente desde Audit Vault, reduciendo el costo de seguridad de IT.

Oracle Audit Vault recopila y consolida transparentemente los datos de auditoría, brindando conocimientos valiosos sobre *quién* hizo *qué* a *cuáles* datos y *cuándo*– incluidos los usuarios privilegiados que tienen acceso directo a la base de datos. Con los informes, las notificaciones de alerta y la administración centralizada de políticas de auditoría de Oracle Audit Vault, el riesgo de amenazas internas y el costo de cumplimiento se ven ampliamente reducidos. Oracle Audit Vault aprovecha la tecnología Oracle de data warehousing y seguridad de datos líder en la industria para administrar, almacenar y archivar grandes volúmenes de datos de auditoría.

Información Simplificada de Cumplimiento

Oracle Audit Vault ofrece informes estándar de evaluación de auditorías que abarcan usuarios privilegiados, administración de cuentas, roles y privilegios, administración de objetos y administración del sistema en toda la empresa. Los informes controlados por parámetros pueden definirse mostrando la actividad de inicio de

sesión del usuario a través de múltiples sistemas y dentro de períodos específicos, como los fines de semana. Oracle Audit Vault brinda un esquema abierto de depósito de auditoría que puede accederse desde Oracle BI Publisher, Oracle Application Express o cualquier herramienta de información de terceros.

Detección Proactiva de Amenazas con Alertas

Los alertas de eventos de Oracle Audit Vault ayudan a mitigar el riesgo y protegerse de amenazas internas al ofrecer notificaciones proactivas sobre actividades sospechosas en la empresa. Oracle Audit Vault monitorea continuamente los datos de auditoría entrantes, evaluando los datos de auditoría frente a las condiciones de alerta. Los alertas pueden asociarse con cualquier evento de base de datos auditable, incluso eventos del sistema como los cambios en las tablas de aplicaciones, el otorgamiento de roles y la creación de usuarios privilegiados en sistemas sensibles. Oracle Audit Vault proporciona resúmenes gráficos de las actividades que provocan los alertas.

Seguridad y Escalabilidad

Proteger los datos de auditoría es crítico para los procesos de seguridad y controles internos. Oracle Audit Vault protege los datos de auditoría al utilizar controles sofisticados, incluidos Oracle Database Vault y Oracle Advanced Security. El acceso a datos de auditoría dentro de Oracle Audit Vault está estrictamente controlado. Los usuarios DBA privilegiados no pueden ver ni modificar los datos de auditoría. Incluso se evita que los auditores modifiquen los datos de auditoría. Oracle Audit Vault aprovecha las capacidades probadas de Oracle para data warehousing y particionamiento a fin de alcanzar escalabilidad masiva, un requisito clave para cualquier solución de auditoría. Oracle Audit Vault puede opcionalmente implementarse con Oracle Real Application Clusters (RAC), permitiendo la escalabilidad, la alta disponibilidad y flexibilidad.

Costos Más Bajos de IT con las Políticas de Oracle Audit Vault

El personal de seguridad de IT trabaja con los auditores para definir los parámetros de auditoría en las bases de datos y otros sistemas de la empresa con el fin de cumplir con los requerimientos de cumplimiento y las políticas de seguridad interna. Oracle Audit Vault ofrece la capacidad de suministrar y revisar los parámetros de auditoría en múltiples bases de datos desde una consola central, reduciendo el costo y la complejidad de administrar los parámetros de auditoría en toda la empresa.

Oracle Enterprise Manager Configuration Management Pack

Oracle Enterprise Manager Configuration Management Pack proporciona una solución valiosa, basada en políticas, para la detección de vulnerabilidades. Ofrece evaluaciones automatizadas para las configuraciones seguras mediante soluciones de políticas basadas en XML para listas de control de seguridad, puntos de referencia de configuración, pruebas automatizadas de cumplimiento y resultado de cumplimiento. Oracle Enterprise Manager Configuration Management Pack incluye más de 240 políticas "ejemplo" en áreas como seguridad, configuración y almacenamiento. Las políticas ayudan a una continua evaluación de seguridad por medio de la detección automatizada de vulnerabilidades críticas de seguridad.

Las políticas son efectivas en la administración de cambios de configuración (a través de la instalación de parches, la incorporación de archivos y directorios, el cambio de parámetros y puertos, editar sus dependencias, etc.) al auditar continuamente frente a configuraciones prescriptas. Este "cambio" es rastreado de manera que los administradores sepan cuándo suceden, qué cambios son aceptables y qué cambios deben corregirse. Este nivel de seguridad y cumplimiento, a través de la auditoría y la ejecución proactivas, es necesario para mantener el control en la inestabilidad continua que define a la mayoría de los centros de datos actuales. Las políticas pueden programarse y aplicarse de acuerdo con los objetivos.
Aumentar el cumplimiento regulatorio exige que los sistemas de IT sean seguros y no hayan estado comprometidos. Asegurar que los sistemas de IT estén en línea con

las mejores prácticas de seguridad es crítico para cualquier negocio de IT. Los Grupos de Políticas (un grupo de políticas de seguridad y configuración que se equipara a un estándar regulatorio o de mejores prácticas) permiten que los administradores y CIOs obtengan una vista rápida de cómo sus sistemas cumplen con las mejores prácticas de seguridad especificadas en su entorno. Estos resultados de evaluación se convierten en valores de cumplimiento (de acuerdo con un promedio ponderado) y los valores generales pueden presentarse en un tablero de control de cumplimiento. El tablero presenta resúmenes de indicadores clave, con la capacidad de desglosar a detalles, permitiendo que los usuarios monitoreen y verifiquen continuamente su postura de cumplimiento. El soporte de análisis de tendencias ofrece la capacidad de rastrear el progreso hacia el cumplimiento a lo largo del tiempo para todo el entorno de IT. Las excepciones y violaciones pueden remediarse para lograr que los sistemas vuelvan a estar en conformidad con los grupos de políticas.

Manage Policy Library

Revert

Previous 1-25 of 45 N

Priority	Policy Rule	Category	Target Type	Description	Disable	D B
	Well-known accounts	Security	Database	Test for accessibility of well-known accounts		
	Web Cache Writable files	Security	Web Cache	Check that there are no group or world writable files in the Document Root directory.		
	Web Cache owner and setuid bit'	Security	Web Cache	Check that webcached binary is not owned by root and setuid is not set		
	Web Cache Dummy wallet	Security	Web Cache	Check that dummy wallet is not used for production SSL load.		
	Web Cache Access Logging	Security	Web Cache	Check that Web Cache access logging is enabled		
	Users with System Tablespace as Default Tablespace	Storage	Database	Checks for non-system users using SYSTEM or SYSAUX as the default tablespace		
	Users with Permanent Tablespace as Temporary Tablespace	Storage	Database	Checks for users using a permanent tablespace as the temporary tablespace		
	Use of Unlimited Autoextension	Storage	Database	Checks for tablespaces with at least one datafile whose size is unlimited		
	Use of Non-Standard Initialization Parameters	Configuration	Database	Checks for use of non-standard initialization parameters		
	Unlimited login attempts	Security	Database	Check for limits on the number of failed logging attempts		

Figura 9. Enterprise Manager Configuration Management Pack – Políticas de Configuración Segura

RESUMEN

Las soluciones transparentes de seguridad son críticas para la actual economía de negocios globales. Cubrir el cumplimiento regulatorio y reducir el riesgo de las amenazas internas requiere una sólida seguridad sobre los datos de aplicaciones. Modificar el código de aplicaciones existentes puede ser un proceso complejo y costoso. Los productos de Oracle Database Security están diseñados para trabajar de manera transparente, minimizando cualquier impacto sobre las aplicaciones existentes y cumpliendo con los mandatos regulatorios de muchas regulaciones.

Oracle Database Vault cumple de manera transparente con los estrictos requerimientos de controles internos de SOX, PCI, HIPAA y muchas otras regulaciones. Oracle Database Vault Realms evita que incluso el DBA acceda a información financiera sensible o relacionada con la privacidad que se puede encontrar en las aplicaciones. Las etiquetas de sensibilidad de Oracle Label Security ofrecen una gran cantidad de nuevos factores para utilizar en las decisiones de autorización de factores múltiples de Oracle Database Vault. La encriptación de datos transparentes de Oracle Advanced Security brinda una solución atractiva para la encriptación PCI y los requisitos de administración clave, y sigue liderando la industria de encriptación con encriptación LOB y de espacio de tabla en Oracle Database 11g. Oracle Audit Vault convierte los datos de auditoría en un recursos de seguridad clave, consolidando y asegurando transparentemente la información de auditoría vital asociada con la actividad de base de datos. Los informes, alertas y políticas de Oracle Audit Vault aceleran la tarea de los funcionarios de seguridad y el personal de cumplimiento de auditoría. Oracle Enterprise Manager Configuration Management Pack monitorea continuamente las bases de datos y los hosts para encontrar violaciones a la seguridad y mejores prácticas de configuración, simplificando así en gran medida la tarea del administrador de seguridad.

Oracle Database 11g versión 1 Soluciones Transparentes para Seguridad y Cumplimiento
Junio de 2007
Autor: Paul Needham
Coautor: Kamal Tbeileh

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.