Cómo satisfacer requerimientos regulatorios de Seguridad de Información con la base de datos Oracle

Autor: Lina Forero

White Paper, rP. Copyright © abril 2010, redPartner S.A. Todos los derechos reservados.

Índice

White Paper, rP. Copyright © abril 2010, redPartner S.A. Todos los derechos reservados.

Introducción

Las mejores prácticas de Seguridad Informática consideran tres aspectos principales de la Seguridad de la Información:

1. Confidencialidad: Protección en contra del acceso no autorizado a la información.

2. Integridad: Prevención de las modificaciones no autorizadas de la información.

3. Disponibilidad: Prevención y recuperación de errores en hardware y de ataques de negación de acceso.

I. Las Bases de Datos y Seguridad de la Información

Los componentes de seguridad que ofrece una base de datos se dividen en las siguientes categorías:

Autenticación

Mecanismo para identificar a los usuarios y confirmar su identidad.

Control de Acceso

El mecanismo de control de acceso proporciona Integridad y Confidencialidad de la información mediante la definición de privilegios y permisos de acceso por perfiles de usuario a la información.

Protección de los Datos

Adicionalmente al control de acceso, técnicas de encripción para los datos almacenados o en tránsito proporcionan protección adicional.

Monitoreo (Auditoría)

Toda acción que sea relevante desde el punto de vista de la Seguridad debe ser registrada para comprobar la eficacia de los controles existentes y poder recomendar cambios en la política de seguridad cuando sea necesario.

White Paper, rP. Copyright © abril 2010, redPartner S.A. Todos los derechos reservados.

II. ISO 27001

Este estándar internacional promueve la adopción de una aproximación mediante procesos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Información para la Administración de la Seguridad de Información de una organización (Information Security Management System - ISMS).

Una organización necesita identificar y administrar muchas actividades para funcionar adecuadamente. Cualquier actividad que utilice recursos y sea manejada de forma que permita transformar las entradas en salidas puede considerarse como un proceso. A menudo, la salida de un proceso se convierte en la entrada para otro proceso.

El foco de la norma ISO/IEC 17799:2005, la precursora de la ISO 27001, es garantizar la disponibilidad, confidencialidad e integridad de la información de la organización. Estos principios están en el corazón de cualquier regulación relacionada con la información.

ISO 27001 está reconocida internacionalmente como una metodología estructurada para la Seguridad de Información. Ahora, la ISO 27001 no exige procedimientos específicos ni las técnicas de implementación a seguir para obtener la certificación.

Dependiendo de la Política de Seguridad de la Información de la compañía y sus necesidades particulares, se deben diseñar controles adecuados que permitan alcanzar el objetivo, bien sea esta una certificación o el cumplimiento de mejores prácticas en el tema de Seguridad de Información.

Las compañías que utilizan Oracle para almacenar sus datos, tienen a su disposición características sofisticadas como *Virtual Private Database* y *Fine Grain Auditing* para apoyar sus esfuerzos de implementación de controles adecuados, garantizando que se preserva la Confidencialidad, Integridad y Disponibilidad de la Información contenida en su base de datos.

A continuación una breve descripción de Oracle VPD, una tecnología disponible para bases de datos Oracle Enterprise Edition.

White Paper, rP. Copyright © abril 2010, redPartner S.A. Todos los derechos reservados.

III. Oracle Virtual Private Database

Virtual Private Database (VPD), es una característica sin costo adicional de la base de datos Oracle Enterprise Edition, que fue introducida desde Oracle8*i*.

VPD permite implementar controles para satisfacer requerimientos de seguridad cuando los privilegios y roles estándar no son suficientes. Las políticas VPD pueden ser simples o complejas dependiendo de sus requerimientos. VPD puede usarse en combinación con "contextos de aplicación" para implementar requerimientos de seguridad a nivel de filas y/o columnas para cumplir así requerimientos regulatorios.

Contextos de Aplicación

Un contexto de aplicación es un conjunto de tuplas nombre-valor que la base de datos Oracle almacena en memoria. Un contexto de aplicacion está asociado a una etiqueta, o namespace, por ejemplo: empno_ctx para un application context que consulta los IDs de los empleados.

Una aplicación puede usar el contexto de aplicación para acceder a información de sesión acerca de un usuario, como por ejemplo el ID de la máquina cliente que luego puede pasarse de manera segura a la base de datos.

Una política simple de VPD puede restringir acceso a los datos únicamente durante el horario de oficina; un ejemplo más sofisticado puede leer un contexto de aplicación para establecer un esquema de seguridad de acceso a nivel de filas para la tabla de Pedidos. Aquí el contexto de aplicación proporciona la información acerca del usuario que se está conectando a la base de datos para que la política pueda filtrar los datos de acuerdo a sus privilegios.

Sin importar como los usuarios se conectan a la tabla protegida (vía una aplicación, una interfaz Web or SQL*Plus), el resultado es el mismo. No existe un "problema de seguridad en la aplicación" puesto que la política de acceso está asociada a la tabla y no puede evitarse.

White Paper, rP. Copyright © abril 2010, redPartner S.A. Todos los derechos reservados.

CUST_FIRST_NAME	CUST_LAST_NAME	CUSTOMER_ID
Matthias	Hannah	106

ORDER_DATE	CUSTOMER_ID	ORDER_TOTAL
31-AUG-99 09.19.37.811132 AM	105	22150.1
20-MAR-96 05.18.21.862632 PM	106	5546.6
01-AUG-00 10.22.48.734526 AM	106	2075.2
31-AUG-99 08.53.06.008765 PM	107	70576.9

Ejemplo: Un cliente solo puede ver sus pedidos en la tabla de pedidos (arriba), cuando aparece en la tabla de clientes (abajo)

Oracle Database 10g adicionó nuevas características a Virtual Private Database: con "Column Relevance", VPD puede configurarse de forma tal que la política entre en efecto **sólo** cuando una columna crítica es seleccionada:

CUST_LAST_NAME	CUST_FIRST_NAME	ACCOUNT_MGR_ID
Roberts	Ishwarya	145
Steenburgen	Gustav	145
Olin	Hal	147
Kanth	Hannah	147
Seignier	Blake	149
Powell	Claude	149

CUST_LAST_NAME	CUST_FIRST_NAME	CREDIT_LIMIT	ACCOUNT_MGR_ID
Seignier	Blake	1200	149
Powell	Claude	1200	149

Ejemplo: El gerente de cuenta con id "149" puede ver todas las filas de la tabla de clientes, pero no sus límites de crédito. Tan pronto como ella consulta la columna 'credit_limit', únicamente tiene acceso a sus propios clientes.

La configuración más avanzada ("Column Hiding") de VPD facilita la combinación de facilidad de uso y seguridad: Ella continúa teniendo acceso a la tabla de 'clientes', pero la información confidencial permanece oculta:

White Paper, rP. Copyright © abril 2010, redPartner S.A. Todos los derechos reservados.

CUST_LAST_NAME	CUST_FIRST_NAME	CREDIT_LIMIT	ACCOUNT_MGR_ID
Edwards	Guillaume		145
Mahoney	Maurice		145
Warden	Maria		147
Landis	Marilou		147
Dvrrie	Rufus		148
Belushi	Rufus		148
Seignier	Blake	1200	149
Powell	Claude	1200	149

Ejemplo: Todas las columnas de 'credit_limit' están vacías excepto aquellas de sus propios clientes.

Oracle VPD es la tecnología sobre la que se fundamenta el producto Oracle Label Security, que es una opción para la base de datos Oracle Enterprise Edition introducida con Oracle 8.1.7. Oracle Label Security permite o niega el acceso a filas de datos comparando la 'etiqueta' (label) de una fila con el conjunto de 'etiquetas' o labels del usuario.

Ejemplos de niveles de sensibilidad incluyen:
1. Interno
2. Confidencial
3. Directivos únicamente
4. Altamente Sensibles
5. Presidencia
6. Confidencial - Operación XYZ
7. Sensible : Finanzas - Latinoamérica
8. Top Secret
9. No clasificado

IV. Cómo se Compara Oracle Virtual Private Database (VPD) con Oracle Label Security?

Oracle VPD ofrece excelentes funcionalidades de seguridad – control de acceso granular (FGAC), contextos de aplicación y contextos globales.

Las políticas de VPD se escriben utilizando PL/SQL, y pueden ser asignadas a vistas o tablas individuales. Las consultas que referencien tablas y vistas protegidas por VPD.

Las políticas de VPD pueden restringir el acceso comparando el valor de un atributo en una fila individual con un valor del contexto de la aplicación.

White Paper, rP. Copyright © abril 2010, redPartner S.A. Todos los derechos reservados.

Oracle Label Security es una solución lista para seguridad a nivel de fila, basada en la tecnología de VPD. No se requiere escribir código ni desarrollar software, permitiendo que el administrador se concentre exclusivamente en la política.

Oracle Label Security proporciona una interfaz para crear políticas, especificando opciones de exigencia, definiendo etiquetas de sensibilidad de datos, estableciendo etiquetas de autorización de usuarios, y protegiendo tablas y esquemas individuales.

Las etiquetas de sensibilidad de datos proporcionan un mecanismo muy flexible y poderoso para restringir el acceso a los datos. Por ejemplo, los datos pertenecientes a diferentes organizaciones o compañías puede separarse utilizando etiquetas de sensibilidad y compartirse de manera selectiva cambiando dinámicamente las etiquetas de sensibilidad.

Dependiendo de la complejidad de la política de seguridad, Oracle Virtual Private Database (VPD) podría ser preferible para la implementación. Adicionalmente, Oracle Label Security es ideal para situaciones en las cuales las decisiones de control de acceso necesitan basarse en la sensibilidad de la información.

Oracle VPD es una funcionalidad incluida en Oracle Enterprise Edition sin costo adicional. Oracle Label Security una opción adicional con costo de licenciamiento ,para Oracle Enterprise Edition.

Para implementar políticas de seguridad asociadas a sus datos en la base de datos Oracle, redPartner ofrece servicios de Consultoría en el diseño e implementación de la solución.

White Paper, rP. Copyright © abril 2010, redPartner S.A. Todos los derechos reservados.

V. Bibliografía

1. Documentación pública de Oracle: http://www.oracle.com/technology/deploy/security/database-security/virtual-private-database/index.html

2. Oracle White Paper: "Oracle Label Security for Privacy and Compliance." http://www.oracle.com/technology/deploy/security/databasesecurity/pdf/twp_security_db_label_privacy_11gr1_20070623.pdf

3. Bertino, E., Byun J. and Kamra, A. Database Security.In *Security, Privacy and Trust in Modern Data Management.* Petkovic, Milan; Jonker, Willem (Eds.)2007, capítulo 7.

VI. Acerca de redPartner

redPartner es una empresa con presencia en Ecuador y Perú, que desde junio del 2004 se ha dedicado a ayudar a construir sistemas informáticos que tengan sentido estratégico y de negocios para sus clientes.

Brindando la mejor Tecnología de Información redPartner distribuye productos de importantes líneas como Oracle, Symantec, Redhat, Citrix, HP y Google. El éxito de la empresa está directamente relacionado con el de nuestros clientes, redPartner busca apoyarlos para que Tecnología de Inteligencia sea un habilitador de su estrategia de negocios.

VII. Sobre el Autor

Lina Forero actualmente es Gerente de Consultoría de redPartner, posee el título de Master of Science in Computer Science de la Universidad de Illinois en Urbana - Champaign.

Con más de 15 años de experiencia en soluciones Oracle, coordinando equipos de desarrollo, consultoría y soporte técnico. Además ha trabajado en Oracle Consulting en Oracle Corp.-Colombia y es instructora de Oracle University. Certificada en Information Assurance de acuerdo a la norma NSTISSI 4011.

White Paper, rP. Copyright © abril 2010, redPartner S.A. Todos los derechos reservados.

Retroalimentación

Nos interesa mucho su opinión y retroalimentación. Solo con la retroalimentación de nuestros clientes podemos mejorar este documento y nuestros servicios. Desde ahora agradecemos y apreciamos mucho sus comentarios.
Por favor escríbanos a: *contacto@red-partner.com*

Copyright
Copyright © abril 2010, redPartner S.A. Todos los derechos reservados. All rights reserved. Este documento tiene propósitos informativos únicamente. Su contenido puede ser modificado sin previo aviso por parte de redPartner. Este documento no puede ser considerado como un compromiso contractual explícito o implícito. Además no puede ser reproducido o transmitido por ninguna forma o formato bajo ninguna circunstancia, sin el permiso previo y expreso.
redPartner es una marca registrada por redPartner S.A. Otros nombres son marcas de sus respectivos dueños.13/04/2010

redPartner Perú S.A.C
Monte Rosa 255 Piso 4,
Chacarilla – Surco, Lima