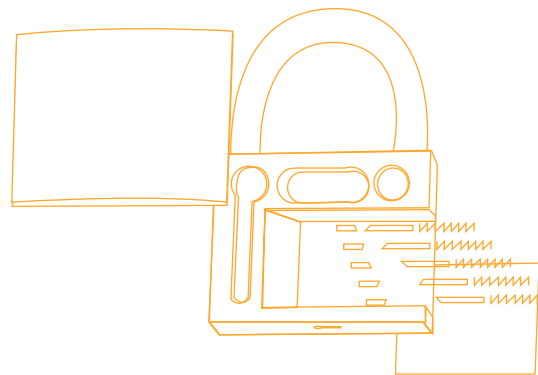




Oracle Selective Audit



Oracle Selective Audit.

Con un interfaz gráfico de usuario (GUI) fácil de usar, Selective Audit es la solución definitiva a las necesidades de auditoría, monitorización y cumplimiento de la LOPD.

Selective Audit está basado en Java y puede utilizarse sobre bases de datos Oracle independientemente de donde estén instaladas.

LA NECESIDAD DE AUDITORÍA DE SEGURIDAD

En la actualidad, las empresas almacenan cada vez más datos sensibles: información de clientes y personas, información estratégica, planes, investigaciones, etc. La custodia de este tipo de información es una necesidad y una obligación, llegando en algunos casos a ser exigida por la ley. Si bien es importante el acceso restringido a esta información sensible por alguien no autorizado, es imprescindible tener la capacidad adicional de detectar si se ha realizado un acceso autorizado pero no adecuado, quién lo ha hecho y qué información se ha comprometido.

Es más, el objetivo definitivo es obtener un nivel de seguridad que nos permita responder categóricamente a la pregunta: *¿Se ha realizado algún acceso no autorizado desde mi sistema?*

ABORDAR LA AMENAZA DEL "INSIDER" (USUARIO INTERNO)

Una de las amenazas principales a la seguridad de la información viene del "insider" (usuario interno). De manera consecuente, varios estudios de seguridad han documentado que más del 70% de las pérdidas de datos de los sistemas de información y ataques han sido perpetrados por "insiders" –los autorizados al menos con algún nivel de acceso al sistema y sus datos. La mayoría de las tecnologías de seguridad, de cualquier forma, están diseñadas para asegurar los datos ante ataques externos. Una de las razones principales para este énfasis es que proteger el acceso a los sistemas de los "outsiders" (agentes externos) es a la vez más fácilmente comprensible y técnicamente menos desafiante o problemático. Nótese que, una vez que un "outsider" ha penetrado en un sistema y ha suplantado la identidad de un usuario autorizado, se convierte en un "insider". Protegerse contra la actividad no autorizada de "insiders" requiere aproximaciones diferentes.

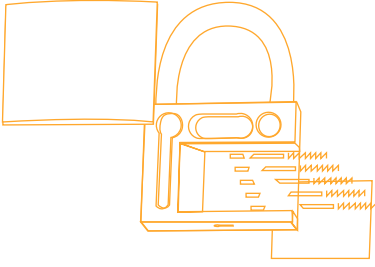
Si definimos lo que podemos considerar como un comportamiento "normal" es posible diseñar y reforzar una política de auditoría enfocada a la detección y alerta en la dirección de los intentos sospechosos de acceder a los datos dentro del sistema, que se apartan de ese comportamiento.

Saber qué es un comportamiento "normal", ha sido siempre un desafío. Las técnicas de análisis y las tecnologías no están preparadas para soportar el desarrollo de perfiles de acceso de los usuarios a los datos. Para tratar esta deficiencia, el Advanced Program Group de Oracle ha desarrollado una solución llamada "Selective Audit", única en su capacidad de realizar análisis de acceso y manipulación de datos dentro de las bases de datos Oracle, construir patrones de comportamiento de los usuarios, e identificar accesos no autorizados a los datos.

En este caso, el objetivo es la respuesta a la pregunta: *¿conozco el uso real que mis usuarios hacen de sus privilegios?*

LA SEGURIDAD EN ORACLE Y SELECTIVE AUDIT

La base de datos Oracle proporciona un rico conjunto de capacidades de seguridad de forma nativa. Éstas incluyen el uso de dominios de seguridad, privilegios para el control de acceso discrecional, roles, encriptación y auditoría. Oracle también tiene funcionalidades en tecnología de seguridad que proporcionan encriptación de datos y control de acceso obligatorio.



Solutions PACK
Oracle Selective Audit

El uso efectivo de estas características de seguridad es clave para asegurar que los datos están protegidos.

De cualquier manera, determinar qué elementos auditar, establecer la configuración de auditoría y revisar los datos de la auditoría generada por una base de datos con cientos o miles de usuarios es una tarea desalentadora. La carga de este esfuerzo y el volumen de datos, llevan normalmente, a una circunstancia en la que la auditoría es realizada a menudo de forma ineficaz o inconclusa –incluso por agencias que tienen la obligación de auditar.

La solución Selective Audit con un interface gráfico usuario intuitivo (al estilo de Oracle Enterprise Manager) reduce la carga de establecer medidas efectivas de auditoría y es una poderosa herramienta de administración del sistema de auditoría que ayuda en la planificación y gestión de más de 250 acciones de auditoría.

Genera sentencias SQL de auditoría, informes gráficos de análisis y proporciona un incremento significativo del nivel de control sobre lo que es auditado, con un mayor grado de granularidad. De este modo, el volumen de traza generado puede ser drásticamente disminuido mediante el filtrado selectivo de registros a auditar.

En definitiva, nos permite convertir el tradicional listado de infinitas líneas de trazas de auditoría, en información interpretable, y más aún, en conocimiento útil sobre el comportamiento de mi sistema.

Usando Selective Audit, los directores de seguridad podrán auditar accesos específicos a bases de datos y acciones de manipulación de datos orientados a:

- La sensibilidad de los datos accedidos (básico, medio, alto)
- La identidad del usuario (usuarios genéricos y usuarios físicos)
- Valores concretos de atributos (registros de especial protección)

Selective Audit está orientado a conseguir un mínimo impacto en los sistemas existentes, con el beneficio adicional de un rápido proceso de implantación.

Requisitos de Hardware y Software

Base de Datos Oracle9i sobre cualquier plataforma y sistema operativo soportado. Con algunas limitaciones funcionales sobre Oracle8i.

CARACTERÍSTICAS DEL INTERFAZ DE USUARIO

- Facilidad de uso.
- Configuración y cambios de manera rápida e intuitiva.
- Capacidad de administración centralizada.
- Generación de informes y gráficos.

FUNCIONALIDADES GENERALES

- Más de 250 acciones de auditoría ya definidas.
- Almacenamiento de Informes de Análisis de Auditoría.
- Generación de Sentencias SQL de auditoría.
- Generación de base de datos de auditoría.
- Auditoría por sentencia, privilegio, objeto o usuario.
- Auditoría de ejecución de sentencias exitosas o no.
- Soporte al cumplimiento de la LOPD

Más información y contacto en:

http://www.oracle.com/es/consultoria/oc_solutions_packs

916 312 328

ocospain_es@oracle.com

ORACLE