Universidad de Buenos Aires
Facultades de Ciencias Económicas,
Ciencias Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

TRABAJO FINAL DE MAESTRIA

Título

Configuración y análisis de registros de eventos de auditoria en los sistemas de gestión de base de datos relacional

Autor:
Stella Maris Vilca

Director:
Ingeniero Alberto Dams

Año de presentación: 2018

Cohorte: 2010

Declaración Jurada de origen de los contenidos

Por medio del presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis o Trabajo Final de Maestría vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Stella Maris Vilca
DNI 23.611.082

Resumen

En el presente trabajo, se efectúo una investigación sobre las modalidades que proveen Oracle, SQL Server, SAP ASE y Teradata para habilitar el registro de eventos de auditoria y se analizó el contenido de los eventos registrados.

Al respecto, se identificó que la configuración del registro de eventos de auditoria se realiza de una forma diferente en cada uno de los sistemas de gestión de base de datos relacional y que para no comprometer la disponibilidad del servicio es primordial habilitar únicamente el registro de los eventos críticos.

Además, en todos los productos fue factible interpretar satisfactoriamente el contenido de los eventos registrados. Sin embargo, se considera que la tarea de análisis tiene un alto costo operativo debido a la heterogeneidad de los datos y el uso de una herramienta específica para el análisis facilita dicha tarea y permite la detección oportuna de los eventos críticos.

Adicionalmente, se describen los proyectos ejecutados en una organización que incrementaron sus niveles de seguridad a través de la configuración y el análisis de los registros de eventos de auditoría de Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10 y la implementación de una herramienta específica para el análisis de eventos críticos

Finalmente, se informa que la metodología empleada es descriptiva y exploratoria y las fuentes de documentación utilizadas son directas o primarias.

Palabras claves

Sistema de gestión de base de datos relacional – registro de eventos de auditoria – configuración – análisis

Indice

Cuerpo Introductorio 1
Capítulo I 3
1.1 Definiciones 3
1.1.1 Registros de eventos de auditoria 3
1.1.2 Funciones del almacenamiento de eventos 4
1.1.3 Funciones del análisis de eventos 5
1.1.4 Funciones de la depuración de eventos 5
1.1.5 Procesos operativos de la gestión de los registros de eventos de auditoria 5
1.2 Configuración y análisis de registros de eventos de auditoria en Teradata 9
1.2.1 Reglas de registro de eventos 10
1.2.2 Tablas BDQL, vistas y macros 12
1.2.3 Almacenamiento y protección de los datos de las consultas 13
1.2.4 Análisis de los datos de BDQL 14
1.2.5 Tablas temporales DBQL y tablas históricas DBQL 15
1.2.6 Revisión de las reglas de registro 15
1.3 Configuración y análisis de registros de eventos de auditoria en SAP Adaptive Server Enterprise 15
1.3.1 Instalación del registro de eventos de auditoria 16
1.3.2 Base de datos sybsecurity y tablas sysaudits 17
1.3.3 Configuración del registro de eventos de auditoria 18
1.3.4 Opciones de auditoria 20
1.3.5 Análisis de los registros de eventos de auditoria 22
1.3.6 Consulta de las opciones de auditoria habilitadas 22
1.4 Configuración y análisis de registros de eventos de auditoria en SQL SERVER 22
1.4.1 Distintas modalidades del registro de evento de auditoria 23
1.4.2 Análisis del registro de evento de auditoria 29
1.4.3 Consulta de las opciones de auditoria habilitadas 30
1.5 Configuración y análisis de registros de eventos de auditoria en Oracle 30
1.5.1 Configuración básica 32
1.5.2 Auditar a Sysdba y a los usuarios Sysoper 35
1.5.3 Auditoria unificada 35
1.5.4 Visualización opciones de auditoria 38
1.5.5 Análisis de los registros de eventos 39
Capítulo II 41
2.1 Comparación entre los sistemas de gestión de base de datos relacional 41
2.1.1 Configuración de registros de eventos de auditoria 41
2.1.2 Análisis de registros de eventos de auditoria 45
Capítulo III 49
3.1 Especificaciones del requerimiento 50
3.1.1 Objetivos 50
3.1.2 Participantes 50
3.1.3 Situación actual 50
3.1.4 Problemas actuales 51

3.1.5 Objetivos y Resultados Esperados 51
3.1.6 Alternativas 52
3.1.7 Descripción general de los requerimientos 59
3.1.8 Lista de los requerimientos 59
3.2 Plan de trabajo 61
3.2.1 Antecedentes del proyecto 61
3.2.2 Planeamiento global del proyecto 65
3.2.3 Planeamiento detallado del proyecto 67
3.3 Informe de situación final 74
Capítulo IV 79
4.1 Especificaciones del requerimiento 79
4.1.1 Objetivos 79
4.1.2 Participantes 80
4.1.3 Situación actual 80
4.1.4 Problemas actuales 83
4.1.5 Objetivos y Resultados Esperados 83
4.1.6 Alternativas 84
4.1.7 Descripción general de los requerimientos 85
4.1.8 Lista de los requerimientos 85
4.2 Plan de trabajo 87
4.2.1 Antecedentes del proyecto 87
4.2.2 Planeamiento global del proyecto 88
4.2.3 Planeamiento detallado del proyecto 90
4.3 Informe de situación final 97
Capítulo V 101
Conclusión 103
Anexo I: Opciones de las teglas de registro de eventos de Teradata 111
Anexo II: Detalle de las tablas BDQL, vistas y macros de Teradata 116
Anexo III: Gestión de tablas temporales e históricas DBQL de Teradata 135
Anexo IV: Detalle de la vista DBC.DBQLRulesV de Teradata 136
Anexo V: Ejemplo de procedimiento threshold de Teradata 138
Anexo VI: Opciones de auditoria de SAP Adaptive Server Enterprise 139
Anexo VII: Detalle de sysaudits y sybsecurity de SAP Adaptive Server Enterprise 143
Anexo VIII: Ejemplos de SQL AUDIT de Sql Server 151
Anexo IX: Detalle de los ACTIONS GROUP de Sql Server 153
Anexo X: Contenido de los archivos de extensión trc de Sql Server 158
Anexo XI: Vistas de SQL Audit de Sql Server 162
Anexo XII: Opciones de auditoria por defecto de Oracle 163
Anexo XIII: Comandos a auditar de Oracle 164
Anexo XIV: Tablas con registros de eventos de Oracle 167
Anexo XV: Opciones configuradas para los distintos sistemas de gestión de base de datos relacional 195
Anexo XVI: Cuadro con las opciones de configuración de los sistemas de gestión de base de datos relacional 205
Anexo XVII: Cuadro comparativo del análisis de los registros de eventos de auditoria en los sistemas de gestión de base de datos relacional 216
Anexo XVIII: Ejemplo de registro de evento correspondiente a inicio de sesión 250
Bibliografía 254

Cuerpo Introductorio

El presente trabajo final pretende dar respuestas a las siguientes preguntas: ¿cuál es el objetivo de configurar y analizar los registros de eventos de auditoria en los sistemas de gestión de base de datos relacional?, ¿cómo se lleva a cabo la configuración y el análisis en Oracle, SQL Server, SAP ASE y Teradata?, ¿qué diferencias hay entre estos productos? y ¿cómo se podría implementar estas funcionalidades en una organización?.

Se definió como objetivo general definir los lineamientos para la configuración y el análisis de los registros de eventos de auditoría en los sistemas de gestión de base de datos relacional en una organización específica. Por otro lado, se proponen como objetivos particulares:

- Describir las características técnicas de la configuración y el análisis de los registros de eventos de auditoría para los sistemas de gestión de base de datos relacional: Oracle, SQL Server, SAP ASE y Teradata.
- Comparar las características de la configuración y el análisis de los registros de eventos de auditorías de los sistemas de gestión de base de datos relacional: Oracle, SQL Server, SAP ASE y Teradata.
- Definir los lineamientos para la configuración y el análisis de los registros de eventos de la auditoría para Oracle 12 c, SQL Server 12, SAP ASE 16 SP01 y Teradata 13.10 en una organización específica de acuerdo a los requerimientos de la misma.
- Implementar el análisis de eventos críticos de los sistemas de gestión de base de datos relacional con una herramienta específica.

Para cumplir con los ojetivos mencionados se definió la siguiente estructura en el presente documento:

Capítulo I: corresponde al marco teórico conceptual, incluye las definiciones de los conceptos relevantes y las características técnicas de Oracle, SAP ASE, SQL Server y Teradata relativas a la configuración y análisis de los registros de eventos.

Capítulo II: presenta un análisis comparativo de las distintas modalidades de configuración y análisis de registro de eventos en los sistemas mencionados en el capítulo I.

Capítulo III: describe los lineamientos para la configuración y el análisis de los registros de eventos de auditoría de los productos comerciales: Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10 en una organización específica de acuerdo a los requerimientos de la misma.

Capítulo IV: detalla el proyecto de implementación de una herramienta específica para el análisis de eventos críticos definidos por una organización en particular.

Capítulo V: analiza las vigencias de los lineamientos de configuración y análisis de los registros de eventos de auditoría indicados en el capítulo III y de la herramienta específica para el análisis de eventos descripta en el capítulo IV.

El enfoque utilizado responde al criterio de orientación profesional. Se considera importante especificar que para la lectura del presente trabajo se requiere contar con conocimientos básicos de las características técnicas de los sistemas de gestión de base de datos relacional: Oracle, SQL Server, SAP ASE y Teradata.

Finalmente, se considera que el presente trabajo aporta conocimientos prácticos basados en la experiencia obtenida de participar en proyectos de configuración y análisis de los registros de eventos de auditoría en los sistemas de gestión de base de datos relacional: Oracle, SQL Server, SAP ASE y Teradata. En particular, se brinda información sobre un caso real de implementación que puede ser utilizado en cualquier tipo de organización que requiera disminuir los riesgos, a través de la disponibilidad del registro de las acciones realizadas sobre los los sistemas de gestión de base de datos relacional y la identificación de los eventos que pueden ocasionar posibles incidentes de seguridad. Adicionalmente, se considera un aporte valioso la comparación de la configuración y el análisis de registros de eventos de auditoría entre los distintos productos comerciales analizados.

Capítulo I

1.1 Definiciones

Con el fin de facilitar la comprensión del presente trabajo se detallan a continuación las definiciones consideradas relevantes.

1.1.1 Registros de eventos de auditoria

Un registro de eventos puede tener diversas finalidades, por ejemplo: optimizar los sistemas, realizar un seguimiento del rendimiento o de las acciones de los usuarios [1]. Dichos registros de eventos guardan información de las actividades de los usuarios, excepciones, fallas y eventos de un sistema [2]. En el caso de los sistemas de gestión de base de datos relacional, algunos eventos relativos a los mismos son: la consulta de datos, la eliminación y/o la modificación de datos, la creación, la modificación y la eliminación de los componentes de la estructura de la base de datos y la asignación de permisos a los usuarios, entre otros. Asimismo, según las buenas prácticas en la materia los datos que deberían incluirse en su contenido son:

- identificación unívoca del usuario.
- actividades del sistema.
- fecha y hora de ocurrencia del evento.
- detalle de eventos claves, por ejemplo, inicio y cierre de una sesión.
- identificación unívoca de la terminal y si es posible su ubicación física.
- los intentos exitosos y fallidos de acceso al sistema.
- los intentos exitosos y fallidos de acceso a los datos y otros recursos relacionados al sistema.
- cambios de la configuración del sistema.
- uso de privilegios.
- empleo de utilitarios y aplicaciones del sistema.
- detalle de los archivos accedidos y el tipo de acceso, tales como lectura, escritura o modificación.
- direcciones y protocolos de las conexiones de la red.

- alertas reportadas específicamente por el sistema de control de acceso.
- activación y desactivación del sistema de protección, tales como el sistema de antivirus o el sistema de detección de intrusos.
- Ejecución de las transacciones realizadas por los usuarios en las aplicaciones. [2]

1.1.2 Funciones del almacenamiento de eventos

Rotación: se refiere a la funcionalidad que se presenta cuando se completa un archivo de registro de eventos y se genera uno nuevo. La rotación puede responder a una programación periódica o activarse cuando el archivo de referencia alcanzó un tamaño determinado. Dicha rotación garantiza la preservación de los eventos registrados.

Archivo: esta función corresponde a la retención de los registros de eventos por un tiempo extendido en medios específicos para este fin. Por ejemplo: cintas, almacenamiento SAN o servidores especiales de archivo.

Compresión: consiste en guardar los registros de eventos de una forma que se reduce la cantidad del espacio de almacenamiento y se garantiza que no se produzcan alteraciones en el contenido del archivo. La compresión se efectúa habitualmente cuando los registros de eventos son rotados o archivados.

Conversión: significa transformar en otro formato al registro de eventos original. La conversión incluye acciones tales como filtro, agrupamiento y normalización de los datos.

Normalización: en la normalización de registros, cada campo de datos del registro de eventos se convierte a una representación de datos particular y se clasifica sistemáticamente. La normalización de datos facilita el análisis de múltiples formatos. Uno de los usos más comunes de la normalización es el que se aplica al almacenamiento de fechas y horas en un único formato. Cabe acotar que la normalización puede ser muy costosa en recursos, especialmente por la complejidad de las distintas entradas que pueden presentarse.

Verificación de la integridad: involucra el cálculo de un resumen denominado digesto para cada registro de eventos y el almacenamiento del mismo en

forma segura para garantizar la integridad del mismo. Un digesto es una firma digital que identifica al dato y tiene la particularidad de que un simple cambio de un bit en los datos ocasionaría un digesto completamente diferente. Si el registro de eventos es modificado y su digesto se recalcula, este no coincidirá con el digesto original, indicando que el archivo ha sido alterado. El digesto original debería ser protegido de modificaciones a través de algoritmos de cifrado aprobados internacionalmente, por ejemplo, las recomendaciones de los documentos FIPS o a través de su almacenamiento en dispositivos de sólo lectura u otros mecanismos pertinentes. [1]

1.1.3 Funciones del análisis de eventos

Correlación: significa encontrar relaciones entre dos o más entradas de los registros de eventos. Existen diversas formas de correlacionar los eventos, algunas de ellas son: el empleo de métodos estadísticos o la definición de reglas específicas para detectar determinados patrones.

Visualización: se refiere a la funcionalidad de visualizar los registros de eventos en un formato que pueda ser interpretado por una persona calificada.

Generación de reportes: corresponde a disponer de los mecanismos apropiados para visualizar el análisis de los registros de eventos. [1]

1.1.4 Funciones de la depuración de eventos

Limpieza: esta característica permite remover los registros de un período de tiempo que no se requieren en el presente o ya fueron archivados en otros medios. [1]

1.1.5 Procesos operativos de la gestión de los registros de eventos de auditoria

Configuración del registro de eventos en su origen, incluyendo su generación, almacenamiento y los aspectos de seguridad pertinentes: El administrador deberá identificar que componente de hardware o software participará de la gestión, que tipos de eventos podría generar y que

características o valor registra cada evento. Se destaca que solo debería habilitarse el registro de los eventos relevantes.

En cuanto al almacenamiento y depuración, se recomienda:

- No guardar los datos que no tienen valor para la organización, por ejemplo: mensajes de depuración de desarrollos o aplicaciones.
- Los datos, si es factible, deberían ser guardados en el sistema y también ser trasmitidos a una infraestructura de gestión, con el fin de garantizar la disponibilidad de esta información para su análisis.
- Configurar la rotación, algunas de las opciones son: detener el registro de eventos de auditoria (opción no recomendable desde el punto de vista de seguridad), sobrescribir los datos mas antiguos (esta alternativa es aceptable para los registros de eventos de menor prioridad) o detener el sistema si no se pueden generar los registros de eventos.
- La depuración de los registros de eventos debería garantizar que los eventos mas antiguos sean archivados por el tiempo que se establezca y destruídos cuando ya no sean requeridos.
- Limitar la cantidad de usuarios que acceden a los registros de eventos. Es recomendable que se asigne únicamente permiso de lectura sobre este tipo de datos.
- Evitar que en los registros de eventos se guarden datos sensibles, por ejemplo: las claves de los usuarios.
- Proteger los registros de eventos archivados con mecanismos de cifrado y consideraciones de seguridad física sobre los medios utilizados para las copias de resguardo.
- Implementar mecanismos de seguridad para los registros de eventos en tránsito, por ejemplo: cifrar las comunicaciones utilizadas para su transmisión. [1]

Análisis de registros de eventos de auditoria: El factor clave de éxito para realizar un análisis es entender el contenido de los eventos registrados. En algunos casos, no es factible llevar a cabo esta interpretación, debido a que el software del dispositivo no es capaz de proveer el detalle de un mensaje en particular.

La forma mas efectiva de aprender a analizar los registros de eventos es realizar revisiones y análisis de partes de los registros de eventos periódicamente, por ejemplo, todos los días.

Este proceso es el mayor desafío en la gestión de registros de eventos e implica que se invierta un tiempo considerable. Con el transcurso del tiempo e incremento de los análisis efectuados, se logrará identificar los eventos que representan la actividad normal lo que implicará que las revisiones diarias se realicen en menor tiempo y el análisis se pueda focalizar en los eventos que pueden aportar mayor valor al análisis.

Cabe acotar que el proceso de análisis se puede automatizar en gran medida. Luego de identificar cuales son los eventos interesantes y cuales no, el administrador podría configurar los filtros pertinentes a los registros de eventos para facilitar las tareas de análisis.

Una técnica efectiva es tener dos reportes: uno con los eventos reconocidos y otro con los eventos desconocidos. Ambos reportes deberían ser revisados regularmente, el primero con mayor prioridad que el segundo.

Sin embargo, la revisión frecuente del segundo reporte permitirá que se avance y refine el conocimiento sobre aquellos eventos que aún no se comprenden.

En cuanto a la definición de prioridad de los eventos, se pueden aplicar criterios basados en el tipo de entrada, la frecuencia de aparición, el origen del registro de eventos, el origen o destino de la dirección ip, la hora del día o día de la semana.

La asignación de prioridades también puede incluir la correlación para proveer un contexto de validación de los eventos.

El personal que realiza la revisión y análisis deberá tener conocimientos sobre:

- Las políticas de la organización que definen lo que esta permitido para que se puedan identificar las violaciones o incumplimiento a las mismas.
- El software de seguridad utilizado para detectar los eventos de seguridad de los posibles falsos positivos.
- Las capacidades de registro de los eventos de los componentes de la infraestructura informática. Por ejemplo: interpretar los contenidos de los

registros de eventos del correo electrónico, servidor web, base de datos, entre otros.

- Las características de las técnicas comunes de ataques. En particular, se deberá conocer como estas técnicas se registran en los eventos de los distintos sistemas.
- El software requerido para analizar los registros de eventos. Por ejemplo: herramientas de ejecución de consultas en las bases de datos. [1]

Respuesta a eventos identificados: durante el análisis se pueden identificar eventos significativos, como incidentes o problemas operativos, que requieren de un tipo de respuesta. Por ejemplo: accesos no autorizados a un servidor o un equipo infectado por código malicioso. Cuando se identifique un incidente de seguridad se deberá seguir los procedimientos pertinentes y vigentes en la organización. El personal que analiza los registros de eventos deberá asistir al equipo de respuesta de incidentes, a través de acciones, tales como: ajustar la configuración de captura de registros de eventos para recolectar mayor información o identificar incidentes semejantes en un tiempo corto. [1]

Administración a largo plazo del almacenamiento de los registros de eventos de auditoria: para la administración a largo plazo del almacenamiento de registros de eventos se requiere:

- Elegir un formato para los datos que serán archivados.
- Seleccionar el dispositivo para archivar los registros de eventos, por ejemplo: cintas de backup, CDs, DVDs, almacenamiento SAN y/o servidores de archivos dedicados a este fin. En particular, se debe revisar que el hardware y software requeridos por el medio elegido como almacenamiento esté disponible cuando se necesite recuperar un archivo determinado. Adicionalmente, se deberá revisar periódicamente los archivos resguardados para determinar si se observa algún riesgo de que se transformen en inaccesibles.
- Verificar la integridad de los registros de eventos, esto puede lograrse con el uso de funciones de hashing.
- Definir medidas de seguridad física para los almacenamientos de los registros de eventos, tales como resguardo en áreas seguras, monitoreo de

accesos a dichos sectores, controles del entorno referentes a la humedad, control de temperaturas, protecciones contra las inundaciones, magnetismo u otras cosas que podrían dañar los registros archivados.

- Establecer los mecanismos de destrucción física y lógica de los registros de eventos archivados. [1]

Operaciones de soporte: adicionalmente se podrían efectuar regularmente las siguientes acciones:

- Monitorear que todos los orígenes de captura de registros de eventos estén habilitados, configurados apropiadamente y funcionando de acuerdo a lo esperado.
- Monitorear el proceso de rotación y archivo de los registros de eventos.
- Verificar las actualizaciones y parches en el software empleado en la gestión de los registros de eventos.
- Garantizar que cada sistema tiene su reloj sincronizado con un servicio central y común.
- Ajustar las configuraciones de captura de los registros de eventos de acuerdo a posibles cambios de políticas, modificaciones de tecnologías y nuevas necesidades de seguridad.
- Documentar las anomalías detectadas en la configuración de los registros de eventos y procesos involucrados. [1]

Auditar la gestión de registros de eventos de auditoria: las organizaciones deben realizar actividades periódicas de verificaciones y validaciones para determinar si se cumplen con las políticas, procesos y procedimientos vigentes sobre los registros de eventos. Adicionalmente, se podría revisar el diseño de la infraestructura de gestión de registros de eventos e implementar los cambios necesarios en pos de la mejora continua. [1]

1.2 Configuración y análisis de registros de eventos de auditoria en Teradata

Para elaborar el presente punto se utilizó el manual de administración de Teradata versión 13.10 provisto por el fabricante del producto Teradata Corporation. [3]

En Teradata el registro de eventos de auditoria se realiza con la funcionalidad denominada DBQL. Esta característica utiliza tablas del diccionario de datos predefinidas que se crean en el momento de la instalación del producto. Si no se habilita el registro de los eventos dichas tablas permanecen vacías.

Los pasos para implementar DBQL son:

1. Otorgar el privilegio Execute en el macro DBC.DBQLAccessMacro al usuario que realizará la tarea.
2. Determinar el tipo de información que se quiere registrar.
3. Definir las reglas sobre los datos que se quiere registrar. Las reglas DBQL se pueden aplicar a nivel de usuario, grupo de usuarios, una cuenta, una lista de cuentas o una aplicación.
4. Crear tablas temporales e históricas para el mantenimiento de los datos registrados en la BDQL.
5. Utilizar la sentencia BEGIN QUERY LOGGING para crear el registro de reglas o emplear el comando REPLACE QUERY LOGGING para reemplazar el registro de las reglas existentes con nuevas reglas.
6. Durante las horas de menor actividad, los datos cargados en DBQL se cargan en las tablas temporales de DBC. Se recomienda programar una tarea por la noche para que los registros de DBQL no ocupen espacio en la DBC y de esta forma evitar posibles inconvenientes por falta de espacio.

1.2.1 Reglas de registro de eventos

A continuación, se detalla como se validan las reglas cuando BDQL empieza a registrar los eventos

Paso	**DBQL**
Un usuario inicia sesión	Comprueba el nombre del usuario, el perfil de la cuenta y el nombre de la aplicación en el caché de reglas.
Si se encuentra la regla en el caché	Registra según las opciones de la tabla de reglas.
Si no se encuentra la regla en el caché	Busca los datos en el diccionario de datos.

Si se encuentra en el diccionario de datos	Crea una entrada en el caché de las reglas y registra según las opciones de la tabla de reglas.
Si no se encuentra en el diccionario de datos	Crea una regla “do not log” en el caché de reglas pero no realiza la registración.
Si la regla “"WITH NONE" se encuentra	Crea una regla “do not log” en el caché de reglas pero no realiza la registración.

Para crear una regla que habilita el registro de una sentencia SQL se usan los comandos BEGIN QUERY LOGGING, REPLACE QUERY LOGGING y END QUERY LOGGING. Por ejemplo:

BEGIN QUERY LOGGING WITH SQL ON ALL ACCOUNT='Nombre de la cuenta';

END QUERY LOGGING WITH SQL ON ALL ACCOUNT=' Nombre de la cuenta ';

Se acota que WITH SQL es opcional para la sentencia END QUERY LOGGING.

Se reitera que para ejecutar estas sentencias el usuario debe tener el privilegio de EXECUTE sobre DBC.DBQLAccessMacro.

A continuación, se describen las sentencias en cuestión:

Sentencia	**Propósito**
BEGIN QUERY LOGGING	Habilita el registro de eventos para los usuarios, cuentas o las aplicaciones determinadas.
REPLACE QUERY LOGGING	Reemplaza una regla existente en la tabla DBC.DBQLRuleTbl.
END QUERY LOGGING	Esta sentencia detiene el registro de eventos para los usuarios, cuentas o aplicaciones especificados. Para este caso DBQL llama a una rutina que realiza el commit de los datos y levanta todos los datos de los cachés de DBQL.

Por cada sentencia BEGIN QUERY LOGGING que se habilita, en el momento de inhabilitar dicha regla se debe usar la sentencia END QUERY LOGGING correspondiente. Por ejemplo: si se emplea la sentencia

BEGIN QUERY LOGGING WITH SQL ON user1 ACCOUNT='Marketing';

Para finalizar el registro del usuario Marketing, se debe usar la sentencia

END QUERY LOGGING ON user1 ACCOUNT='Marketing';

Por otro lado, la opción WITH que puede ser utilizada con las sentencias BEGIN/REPLACE QUERY LOGGING habilita registros específicos que se guardan en tablas determinadas. En el Anexo I se presenta un resumen de las distintas opciones de WITH.

1.2.2 Tablas BDQL, vistas y macros

Las tablas BDQL, vistas y macros son los siguientes:

Objeto del diccionario de datos	**Tipo**	**Funcionalidad**
DBQLAccessMacro	Macro	Controla si los usuarios están autorizados a ejecutar la sentencia: BEGIN/REPLACE/SHOW/END QUERY LOGGING
DBQLExplainTbl	Tabla	Contiene la información en una cadena de caracteres sin formato.
DBQLogTbl	Tabla	Guarda filas por defecto.
DBQLObjTbl	Tabla	Guarda una fila por cada objeto referenciado en la consulta.
DBQLRuleCountTbl	Tabla	Guarda la cardinalidad de DBQLRuleTbl (para uso interno solamente)
DBQLRuleTbl	Tabla	Guarda las reglas generadas con BEGIN QUERY LOGGING o REPLACE QUERY La sentencia END QUERY LOGGING remueve las filas de la tabla de reglas. Esta tabla es de uso interno solamente.
DBQLSQLTbl	Tabla	Guarda la totalidad del texto SQL de la consulta. Una consulta puede requerir más de una fila.
DBQLStepTbl	Tabla	Guarda una fila por cada paso del procesamiento usado por una consulta.

DBQLSummaryTbl	Tabla	Guarda consultas que responden al criterio de la regla especificado con la opción SUMMARY o THRESHOLD.
DBQLXMLTbl	Tabla	Guarda el plan XML para todas las sentencias DML.
DBQLRulesV	Vista	Muestra las reglas recientes en DBC.DBCQLRuleTbl.
QryLogV	Vista	Accesos a DBQLogTbl.
QryLogExplainV	Vista	Accesos a DBQLExplainTbl.
QryLogObjectsV	Vista	Accesos a DBQLObjTbl.
QryLogSummaryV	Vista	Accesos a DBQLSummaryTbl.
QryLogStepsV	Vista	Accesos a DBQLStepTbl.
QryLogSQLV	Vista	Accesos a DBQLSQLTbl.
QryLogTDWMV	Vista	Accesos a DBQLogTbl.
QryLogXMLV	Vista	Accesos a DBQLXMLTbl

Adicionalmente, en caso de ser necesario se pueden configurar las vistas que sean necesarias.

En el Anexo II se adjunta la descripción y el detalle de los campos que componen las principales tablas descriptas previamente.

1.2.3 Almacenamiento y protección de los datos de las consultas

Cuando se invoca el registro de una consulta, los datos de la consulta se almacenan en múltiples segmentos del caché de DBQL. Los datos son retenidos hasta que el caché se vacía.

El caché puede ser vaciado en alguna de las siguientes circunstancias:

- Cuando está lleno.
- Ante una sentencia END QUERY LOGGING (con excepción de si se utilizan las opciones summary o threshold).
- Para las opciones SUMMARY o THRESHOLD luego que transcurran 10 minutos.

- Al alcanzar el valor del parámetro DBQLFlushRate (si se incluye las opciones summary o threshold)

Se acota que no hay mecanismos de recuperación para los cachés que colectan las filas de DBQL. Si Teradata es reiniciado, las filas que no han sido enviadas a los AMP se pierden. Sin embargo, el registro de consultas no se detiene, DBQL usa el contenido de la tabla DBQLRuleTbl para continuar registrando.

Las tablas DBQL ocupan permanentemente espacio en la base de datos DBC. Es decir que una única fila enviada a un AMP implica su inserción en DBQL Log para resguardarla a través de la transacción y proceso de recuperación periódico.

Además, los datos en las tablas DBQL se protegen con FALLBACK. Esto significa que el dato esta siempre disponibles al menos en 2 o mas AMPs simultáneamente.

1.2.4 Análisis de los datos de BDQL

El primer nivel de información es capturado en DBQLogTbl y DBQLSummaryTbl. Para consultas de mucho volumen se puede utilizar la opción THRESHOLD en combinación con las opciones SQL, STEPINFO u OBJECTS para reducir la sobrecarga de datos. Además, se pueden especificar las unidades de tiempo transcurrido, uso de CPU o cantidad de entrada/salidas.

Un dato importante para realizar el análisis de datos es el campo CollectTimeStamp. El mismo es registrado en todas las tablas en diferentes puntos del procesamiento del ciclo de la consulta.

Para realizar comparaciones en distintas tablas DBQL se debe obtener el valor del campo QueryID que permite correlacionar los datos.

El análisis de las tablas DBQL requiere conocimientos para realizar consultas SQL y sobre el contenido de las tablas DBQL descriptas en el Anexo II. Por ejemplo, se puede utilizar la herramienta Teradata SQL Assistant y ejecutar la siguiente sentencia para consultar los eventos registrados para el día 27 de julio de 2015:

```
select * from DBC.DBQLogTbl  where cast(starttime as char(10)) ='2015-07-27'
```

1.2.5 Tablas temporales DBQL y tablas históricas DBQL

Por otro lado, se debe tener en cuenta que los datos que se guardan en las tablas DBQL primero se levantan en tablas temporales DBQL y luego pasan a tablas históricas DBQL. En consecuencia, para archivar datos de DBQL se requiere la creación de tablas temporales y tablas históricas. Este tipo de tablas no son tablas de sistemas incluídas en el diccionario de datos y es necesario que sean generadas por el administrador.

Con respecto al mantenimiento, se recomienda limpiar las tablas del diccionario después de copiar los datos relevantes en las tablas DBQL temporales y las tablas DBQL históricas

En resumen, se recomienda la ejecución de los pasos descriptos en el Anexo III.

1.2.6 Revisión de las reglas de registro

La revisión de reglas se puede realizar a través de alguna de las siguientes variantes:

- Utilizar la sentencia SHOW QUERY LOGGING para determinar que regla podría ser empleada por un usuario, cuenta o aplicación. Por ejemplo:

  SHOW QUERY LOGGING ON marketinguser;

  Para ejecutar esta sentencia se requiere el permiso de Execute en DBC.DBQLAccessMacro.
- Consultar la vista DBC.DBQLRulesV que permite visualizar los datos de la tabla DBC.RuleTbl que almacena las reglas en el sistema. Por ejemplo:

  SELECT * FROM DBC.DBQLRULESV WHERE
  ACCOUNTSTRING='$LTest&D&H';

  Para mayor información en el Anexo IV se detallan los campos de la vista DBC.DBQLRulesV.

1.3 Configuración y análisis de registros de eventos de auditoria en SAP Adaptive Server Enterprise

Para elaborar el presente punto se empleo la guía de administración de seguridad de SAP Adaptive Server Enterprise versión 16.0 SP01 [4]

En SAP Adaptive Server Enterprise los componentes del sistema de registro de eventos de auditoria son:

- Base de datos sybsecurity que contiene las opciones globales de auditoria y los registros de eventos que se guardan en las tablas sysaudits.
- La memoria que contiene los eventos antes de que sean escritos en la base de datos sybsecurity.
- Los procedimientos del sistema y los parámetros de configuración que se utilizan para la gestión del registro de eventos de auditoria.

1.3.1 Instalación del registro de eventos de auditoria

Para habilitar el registro de eventos de auditoria se requiere instalar está funcionalidad. En el sistema operativo Unix la instalación se realiza a través de auditinit que se encuentra en el directorio $SYBASE/$SYBASE_ASE/install y el script installsecurity que está disponible en la carpeta $SYBASE/$SYBASE_ASE/scripts. Si el sistema operativo es Windows se debe emplear el script instsecu que se encuentra en el recurso $SYBASE/$SYBASE_ASE/scripts.

Previamente a la ejecución del script se debe realizar la creación de los devices y la base de datos sybsecurity.

En el proceso de instalación se debe definir:

- El número de tablas sysaudits que se utilizarán para el registro de eventos.
- El device que se asigna a cada tabla sysaudits.
- El device para el log transaccional (syslogs). La tabla syslogs existe en todas las bases de datos y contiene el registro de las transacciones que se ejecutan en la base de datos. Para administrar el log transaccional se debe configurar la opción “trunc log on chkpt” en true. Con esta opción el log de la transacción se trunca (todas las transacciones que fueron confirmadas se remueven) cuando el proceso de control verifica que 50 o mas filas han sido escritas en la base de datos (usualmente esto sucede una vez por minuto).

Se acota que el log no se trunca si menos de 50 filas fueron escritas o si el dueño de la base de datos ejecuta manualmente el comando checkpoint. Al instalar la auditoría, esta opción esta activa por defecto. Si

esta opción se desactiva el log puede llenarse y detener el registro de eventos en la sybsecurity.

1.3.2 Base de datos sybsecurity y tablas sysaudits

Debido a que la sybsecurity presenta un nivel intenso de escritura de registros se recomienda:

- No instalar otras tablas en la sybsecurity.
- Ubicar la sybsecurity sobre un disco de uso exclusivo.
- Localizar cada tabla sysaudits sobre su propio segmento o device para que se puedan administrar en forma separada.
- Si los eventos que se registran son críticos se deben implementar device espejados.

Los registros de eventos de auditoria se guardan en tablas de denominadas sysaudits que se encuentran en la base de datos sybsecurity.

Cuando se instala la funcionalidad de auditoria se determina la cantidad de tablas sysaudits. Por ejemplo, si se selecciona tener tres tablas, ellas se llamarán: sysaudits_01, sysaudits_02 y sysaudits_03. La cantidad máxima de tabla es ocho. El fabricante recomienda definir al menos tres tablas y que cada una de ellas tenga un device separado. De esta forma se puede programar un proceso de rotación y almacenamiento de los datos que evite la ocasional pérdida de eventos o la intervención manual para su tratamiento.

Se debe tener en cuenta que para un momento determinado, solo una tabla sysaudits es la que registra los eventos. Dicha tabla se denomina la tabla actual (current audit table). Un usuario con rol SSO puede cambiar la tabla sysaudits que esta capturando los eventos actualmente por otra tabla ejecutando el comando:

Sp_configure “current audit table”, n

[, “with truncate”]

Donde n es un valor entero que determina la nueva tabla. Por ejemplo, 1 equivale a la tabla sysaudits_01. Si el valor es igual a cero significa que la nueva tabla sysaudits es automáticamente la próxima tabla.

La opción with truncate especifica que se truncará la nueva tabla si esta no está completamente vacía. Si no se especifica esta opción y la tabla no está vacía, el comando sp_configure falla. Se debe tener en cuenta que antes de realizar el truncamiento de los datos, estos deben ser resguardados apropiadamente.

1.3.3 Configuración del registro de eventos de auditoria

Previamente a que se habilite la auditoria se debe disponer al menos de tres tablas sysaudits cada una en devices separados, un procedimiento de tratamiento para el umbral (threshold) asociado a cada tabla sysaudits y la configuración pertinente de los parámetros del comando sp_configure. Para ejecutar el comando sp_configure es necesario que el usuario cuente con el rol SSO.

El procedimiento de tratamiento del umbral debe cambiar automáticamente de tabla cuando la tabla que captura actualmente los datos se llena o completa. Se debe contemplar que la próxima tabla está vacía, para ello se debe utilizar el comando sp_configure. Asimismo, los datos de la tabla que está capturando actualmente pueden ser resguardados en otro medio a través de los comandos insert y select. Para asociar dicho procedimiento a cada una de las tablas de auditoria se debe usar el comando sp_addthreshold. Para ejecutar sp_addthreshold se requiere que el usuario sea dueño de la base de datos o System Administrator. Al respecto, se acota que un usuario con el rol SSO puede ser el dueño de la sybsecurity y en consecuencia podría ejecutar sp_addthreshold Por ejemplo, la asociación de un procedimiento denominado audit_thresh a los devices se puede realizar de la siguiente forma:

```
use sybsecurity
go
sp_addthreshold sybsecurity, aud_seg_01, 250, audit_thresh
sp_addthreshold sybsecurity, aud_seg_02, 250, audit_thresh
sp_addthreshold sybsecurity, aud_seg_03, 250, audit_thresh
go
```

Para este ejemplo el procedimiento audit_thresh recibe el control cuando en la tabla de auditoria que captura los eventos actualmente tiene 250 páginas libres. Para mayor información en el Anexo V se presenta un ejemplo de un procedimiento threshold para tres tablas sysaudits.

El comando que se utiliza para configurar el registro de eventos de auditoria es sp_configure y los parámetros relacionados al mismo son:

Auditing: habilita e inhabilita el registro de eventos de auditoria en todo el motor de base de datos. La sintaxis a emplear es la siguiente:

sp_configure "auditing", [0 | 1]

Donde el valor uno representa la habilitación de la auditoria y el valor cero la inhabilitación de la misma.

Auditing queue size: establece el tamaño de la memoria temporal que contiene los eventos antes que sean guardados en el disco. El requerimiento de memoria para un registro simple de auditoria es de 424 bytes. El tamaño por defecto para la memoria temporal es 100 registros o 42 Kb aproximadamente. La sintaxis a emplear es:

sp_configure “audit queue size”, [value]

Donde [value] es el número de registros que la memoria temporal de registros de eventos puede contener. El valor mínimo es 1 y el máximo 65535.

Suspend auditing when full: controla el comportamiento del proceso de auditoria cuando un device se encuentra lleno. La sintaxis a emplear es:

sp_configure "suspend audit when device full", [0|1]

Donde el valor cero significa el truncar la tabla próxima y empezar a utilizar a la misma como tabla de captura de datos. El valor uno indica la suspensión del proceso de auditoria.

Current audit table: define la tabla de auditoria que captura los registros de eventos actualmente. La sintaxis a emplear es:

sp_configure "current audit table", n [, "with truncate"]

Donde n es un valor entero que determina la nueva tabla que va a capturar eventos. Por ejemplo 1 equivale a sysaudits_01, 2 a sysaudits_02, etc. Si se utiliza el valor cero se empleará la próxima tabla, por ejemplo: si en

la instalación se definieron tres tablas, la tabla siguiente es 2 si la tabla actual que captura eventos es sysaudits_01.

La opción "with truncate" especifica que podría truncarse la nueva tabla si esta no está vacía.

1.3.4 Opciones de auditoria

Después que se instaló las funcionalidades básicas de auditoria, se pueden habilitar el registro de eventos en distintos niveles, a saber:

Nivel Servidor	**Nivel Base de Datos**	**Nivel Objeto**	**Nivel Usuario**
Logins Logouts Reboots Remoto procedure Dic commands Security Disk Adhoc	Grant Revoke Truncate Drop Load Create Alter Bcp Bind Unbind Dbaccess Dump	Delete Exec procedure Exec trigger Update Insert Referente Select Update	Cmdtext

Para ello se debe utilizar el comando sp_audit. Para ejecutar esta sentencia se requiere que el usuario cuente con el rol SSO. La sintaxis es:

sp_audit option, login_name, object_name, [setting]

o

sp_audit ‘restart’

Las variantes que puede tener **option** se detallan en el Anexo VI.

login_name: puede tomar los valores: all, un rol de sistema o un login específico.

object_name: *s*e refiere al nombre del objeto que será auditado. Los valores válidos dependen de lo que se especificó en **option**. A saber:

- **All** para todos los objetos
- **Default table**, **default view**, **default procedure**, o **default trigger** para auditar el acceso a cualquier tabla, vista, procedimiento o trigger nuevo. Default table and default view se pueden utilizar cuando el parámetro option

se completó con delete, insert, select, or update. Por otro lado, default procedure es válido cuando se integro el parámetro option con exec_procedure. Default trigger es válido cuando option es igual a exec_trigger.

Setting: *s*e refiere al nivel de registro. Los valores posibles son:

Valor	**Descripción**
on	Activa el registro para una opción especificada.
off	Desactiva el registro para una opción especificada.
Pass	Activa el registro para los eventos exitosos de una opción.
fail	Activa el registro para los eventos fallidos de una opción.

Restart: *s*i el proceso de auditoría se cancela debido a un error se puede reiniciar el proceso de registro de eventos de auditoria con esta opción.

A continuación, se detallan algunos ejemplos de habilitación de registros:

- Todos los eventos relativos a seguridad que fallan o dan error

  sp_audit “security”, “all”, “all”,”fail”

- Todas las acciones de un usuario con rol sa_role

  sp_audit “all”,”sa_role”, “all”,”on”

- Todas las acciones de un usuario con login igual a Tom

  sp_audit “all”, “Tom”, “all”

- Todos los eventos de select sobre tablas denominadas secure-data realizados por el usuario Tom

  sp_audit “select”, “Tom”, “secure-data”

Se debe tener en cuenta que el registro de eventos de auditoria no se activa hasta que se ejecuta la sentencia sp_configure "auditing", 1.

Por otro lado, para agregar registros de eventos de auditoria definidos por el usuario se puede utilizar el comando sp_addauditrecord. La sintaxis es

sp_addauditrecord [text [, db_name [obj_name [, owner_name [,dbid [, objid]]]]]]

Por ejemplo, se podría agregar un registro cuando un usuario desactive la auditoria por reconfigurar el sistema.

sp_addauditrecord @text =’I am disabling auditing briefly while we reconfigure the system”, @db_name= “corporate”

1.3.5 Análisis de los registros de eventos de auditoria

Para consultar el contenido de los registros de eventos de auditoria que se guardan en la base de datos Sybsecurity, el usuario con rol SSO debe utilizar el comando select para ejecutar las consultas. Por ejemplo, si la tabla de la Sybsecurity a consultar es sysaudits_01 y se requiere obtener información de las actividades realizadas por el usuario Bob el 5 de julio de 2015 se deben ejecutar las siguientes sentencias:

```
Use sybsecurity
Go
Select * from sysaudits_01
Where loginname = “Bob”
and eventtime like “Jul 5% 15”
Go
```

Con el fin de facilitar la interpretación del contenido de la tabla sysaudits, en el Anexo VII se brinda el detalle de los campos que la componen, eventos que se registran en la sybsecurity y tipo de datos que se registran en la columna extrainfo de la tabla sysaudits.

1.3.6 Consulta de las opciones de auditoria habilitadas

Para identificar las opciones de auditorias habilitadas se puede consultar la tabla sysauditoptions o ejecutar el comado sp_displayaudit. La sintaxis del comando mencionado es la siguiente:

sp_displayaudit [<procedure>|<object>| <login> | <database> | <global> | <default_object> | <default_procedure> [, <name>]]

1.4 Configuración y análisis de registros de eventos de auditoria en SQL SERVER

Para elaborar el presente punto se utilizó el módulo 12 Auditing SQL

Server Environments del manual del curso 10775A - Administering Microsoft® SQL Server® 2012 Databases provisto por el fabricante [5].

1.4.1 Distintas modalidades del registro de evento de auditoria

El producto SQL Server presenta distintas formas de configurar el registro de eventos de auditoria. Desde SQL Server 2008 versión enterprise se agregó la funcionalidad de SQL Server Audit. Asimimo, se conservan las modalidades de las versiones anteriores. En resumen, las distintas opciones que pueden implementarse en SQL Server 2012 son:

Modo C2 y common criteria: En SQL Server se puede configurar los requerimientos de C2. Esto se realiza a través de la configuración de la opción “c2 audit mode” utilizando el procedimiento almacenado sp_configure. Se debe tener en cuenta que habilitar esta opción puede tener un impacto negativo en el rendimiento del servidor debido a que se genera un gran volumen de eventos. La sintaxis a emplear es:

```
sp_configure 'show advanced options', 1;
GO
RECONFIGURE;
GO
sp_configure 'c2 audit mode', 1;
GO
RECONFIGURE
GO
```

Para ejecutar esta sentencia se requiere que el usuario pertenezca al rol fijo sysadmin.

Los datos se guardan en un archivo en el directorio de datos predeterminado para la instancia (MSQL\Data). Si el tamaño del archivo supera los 200 Mb se crea un archivo nuevo. Este proceso continua hasta que se llene el disco o se desactive el registro de la auditoria.

El fabricante informa que esta funcionalidad se quitará en versiones futuras y será sustituido por common criteria certification.

Adicionalmente, SQL Server provee una opción “common criteria compliance enabled” que puede ser configurada a través del procedimiento almacenado sp_configure. Para ello se debe descargar y ejecutar un script

que finalice la configuración para que SQL Server cumpla con el nivel 4 de Common Criteria Evaluation (EAL4+). Dicho script puede ser descargado del sitio web de Microsoft SQL Server Common Criteria. Cuando se habilita esta opción, se presentan tres cambios en la operación de SQL Server:

Característica	**Descripción**
Residual Information Protection (RIP)	RIP requiere una asignación de memoria para sobrescribir con un patrón conocido de bits antes de que la memoria se reasigne a un nuevo recurso. Cumplir con el estándar RIP puede contribuir a la mejora de la seguridad. Sin embargo, sobrescribir la asignación de memoria puede volver mas lento el rendimiento.
Capacidad para visualizar las estadísticas de los inicios de sesión	Se habilita automáticamente el registro de los inicios de sesión.
El permiso GRANT a nivel de columna no invalida el permiso DENY a nivel de tabla.	Cambia el comportamiento a nivel de permisos del sistema. Un permiso DENY a nivel de tabla tiene prioridad sobre un permiso GRANT a nivel de columna.

SQL Server tiene un inconveniente con la jerarquía de permisos que se mantienen por compatibilidad con versiones anteriores, en el cual un permiso DENY a nivel de una tabla no tiene prioridad sobre un permiso GRANT a nivel de columna. Es decir que se pude denegar a un usuario el acceso a una tabla y si a dicho usuario se le otorga un permiso a nivel de columna de la misma tabla, el usuario puede acceder a la misma.

A continuación, se muestran las sentencias para configurar la opción de common criteria:

```
sp_configure 'show advanced options', 1;
GO
RECONFIGURE;
GO
sp_configure 'common criteria compliance enabled', 1;
```

GO

RECONFIGURE

GO

Para ejecutar estas sentencias se requiere que el usuario tenga asignado los roles fijos de servidor sysadmin y serveradmin.

Empleo de triggers: Antes de la versión de SQL Server 2008 muchas acciones solamente podían ser auditadas a través de triggers. En SQL Server 2005 SP2 se incluyó la funcionalidad denominada logon triggers que se relaciona con el inicio de sesión de un usuario.

Los triggers tienen limitaciones, a saber:

- Impacto en el rendimiento del sistema. A partir de SQL Server 2005, la estructura de las tablas internas empleadas por los triggers fue modificada en un esquema que utiliza tablas que residen en la base de datos tempdb. Los triggers que usan estas tablas operan mas rápido que en las versiones anteriores pero de todas formas pueden tener un impacto significativo en el rendimiento de la base de datos tempdb.

- Pueden ser deshabilitados.

- Tienen un límite de anidación máximo de 32 niveles.

- Los triggers asociados a eventos select no registran los datos que fueron retirados. Este tipo de dato puede ser requerido en entornos de máxima seguridad.

- Hay una capacidad limitada para activar los triggers

Para implementar esta funcionalidad se utilizan las sentencias: create trigger, alter trigger, drop trigger y las tablas de sistema: sys.server_triggers y sys. server_triggers_events.

SQL Trace: El SQL Trace es un conjunto de procedimientos almacenados que son utilizados por SQL Server Profiler. La ejecución de estos procedimientos ofrece un método mas liviano de registro, particularmente cuando los eventos innecesarios se filtran. Muchos usuarios los emplean porque les permite monitorear los comandos que son enviados a SQL Server e identificar los posibles errores. Esta modalidad puede tener un impacto

negativo sobre el rendimiento cuando se ejecuta interactivamente con sistemas productivos.

Desde SQL Server 2005, SQL Trace usa un mecanismo del lado del servidor que garantiza que no se pierden eventos siempre que se disponga de espacio en el disco y que no se observen errores de escritura. Si el disco se llena o se presentan errores de escritura, el registro de la traza se detiene y SQL Server continúa activo a menos que el modo C2 este también habilitado. La posibilidad de pérdida de eventos necesita ser considerada cuando se evalúa el uso de SQL Trace para propósitos de auditoría.

Además de SQL Profiler se puede definir una captura propia de eventos de auditoria mediante el uso de procedimientos almacenados, a través de los siguientes pasos:

1) Especificar los eventos a capturar utilizando sp_trace_setevent
2) Definir los filtros con sp_trace_setfilter.
3) Establecer el destino de los eventos capturados empleando sp_trace_create.

Otros procedimientos almacenados de utilidad son: sp_trace_generateevent (crea eventos definidos por el usuario) y sp_trace_setstatus (modifica el estado de la traza).

Los registros de evento de auditoria se guardan en tablas o archivos de extensión trc.

SQL Server audit: La característica de SQL Server Audit se fundamenta en la funcionalidad denominada Extended Events. Este tipo de eventos permite que se definan acciones a tomar ante la ocurrencia de un evento determinado. Si la acción a seguir está definida, unos eventos son disparados y los detalles del evento son enviados a un lugar específico, por ejemplo: archivos o el registro de eventos de Windows. Se destaca que los Extended Events tienen poco impacto en el rendimiento de la base de datos.

Las configuraciones de los Extended Events son guardadas en paquetes compuestos por archivos de extensión exe o dll. Dichos paquetes no pueden ser modificados, a diferencia de otros paquetes.

Los Extended Events utilizan una terminología específica, a saber:

Objeto	Descripción

Events	Evento de interés durante la ejecución del código.
Targets	Lugar donde el detalle de la traza es enviada.
Actiones	Respuesta al identificar un evento en particular.
Types	Definiciones de los objetos con los que trabaja Extended Events.
Predicates	Filtros dinámicos que son aplicados a los eventos capturados.
Maps	Mapeo de los valores a cadena de caracteres.

Las especificaciones de lo que se audita se determinan a nivel de servidor y a nivel de base de datos. Este conjunto de acciones se conoce como “action groups”. Utilizar un grupo de acciones evita la configuración de un gran número de acciones de auditoría individuales. Algunos ejemplos de actions group son:

BACKUP_RESTORE_GROUP

DATABASE_MIRRORING_LOGIN_GROUP

DATABASE_OBJECT_ACCESS_GROUP

DBCC_GROUP

FAILED_LOGIN_GROUP

LOGIN_CHANGE_PASSWORD_GROUP

Para configurar SQL Server Audit, se deben seguir los siguientes pasos:

1) Crear una auditoría:

Determina como el resultado será procesado. Por ejemplo: definir cuanto tiempo los resultados de la auditoría permanecen en el buffer antes de que se escriban en el repositorio final.

2) Definir el lugar de destino

Determina donde serán enviados los resultados. Se puede guardar los resultados de los registros de evento de auditoría en:

- Un archivo: esta opción brinda el mayor rendimiento y es la más fácil de configurar.
- Registro de aplicación de Windows. Se debe tener en cuenta que este log puede contener información confidencial y cualquier usuario autorizado puede leer su contenido.

- Registro de seguridad de Windows. Esta alternativa es la más segura. Requiere que la cuenta de servicio de SQL Server sea agregada a la política “Generar auditorías de seguridad” antes de que esta pueda ser utilizada. Se debe tener en cuenta que los administradores de la base de datos pueden necesitar acceder a este log.

3) Crear una especificación de la auditoría

Determina las acciones a ser auditadas, tanto a nivel servidor como a nivel de la base de datos. La creación de una especificación de auditoria requiere definir una serie de configuraciones, a saber:

- Nombre de la auditoría
- Demora en cola (en milisegundos): tiempo que SQL Server puede tener en buffer los resultados de la auditoría antes de enviarlas al destino seleccionado. Se debe tener en cuenta que el valor seleccionado debe contemplar la seguridad y el rendimiento del servidor. Por ejemplo, un valor igual a cero ocasionaría que los eventos se escriben al mismo tiempo. Esta configuración permite que no se pierdan eventos ante eventuales fallas pero puede impactar significativamente en el rendimiento del servidor.
- Apagado del servidor ante fallas de la auditoría: indica que SQL Server no puede continuar si la auditoría no está activa.
- Destino de la auditoría.
- Máximo número de archivos a retener.
- Máximo tamaño de cada archivo (MB).
- Espacio del disco reservado para los archivos de la auditoría.
- Máxima cantidad de archivos.

La creación de una especificación de una auditoría a nivel de servidor o a nivel de base de datos puede ser realizada a través de una interface gráfica o con T-SQL. Dichas especificaciones se crean en estado deshabilitado por defecto.

La especificación detalla las acciones a ser auditadas. Se puede seleccionar entre un grupo de acciones o una acción individual y los objetos en cuestión. En el Anexo VIII se presentan algunos ejemplos que facilitan la interpretación.

4) Habilitar la auditoría y la especificación de auditoría

Los permisos que se requieren para habilitar SQL Audit son:

- sysadmin
- permiso CONTROL SERVER
- permiso VIEW SERVER STATE
- permiso ALTER ANY AUDIT
- permiso VIEW AUDIT STATE

En el Anexo IX se adjunta el detalle de los actions groups que pueden aplicarse.

En particular, se acota que un usuario puede agregar eventos de auditoria utilizando el procedimiento almacenado sp_audit_write. Para ello requiere tener asignado el rol public [11].

1.4.2 Análisis del registro de evento de auditoria

La modalidad C2, Common criteria compliance y SQL Trace genera archivos con la extensión trc que contienen los registros de evento de auditoria de SQL Server. Para visualizar su contenido se emplea la herramienta SQL Profiler o la función del sistema sys.fn_trace_gettable.

Para utilizar la función sys.fn_trace_gettable se requiere el privilegio de ALTER TRACE sobre el servidor.

Para el empleo de SQL Profiler para la lectura de los archivos de extensión trc no se necesitan permisos en SQL Server. Solo se requiere que el usuario tenga instalado el aplicativo SQL Server en su computadora.

Los campos del contenido de los archivos de trazas son descriptos en el Anexo X.

Los registros de eventos de auditoria para la modalidad SQL Audit se pueden guardar en distintos destinos. En consecuencia las opciones para su lectura son: acceso a los registro de eventos de Windows, lectura de archivos de registros y consultas a sys.fn_get_audit_file, por ejemplo para el último caso se debe ejecutar la sentencia:

Select * from sys.fn_get_audit_file (‘D:\Audits*’, default, default)

1.4.3 Consulta de las opciones de auditoria habilitadas

Para identificar si el registro de eventos de auditoria tiene implementada la opción C2 o common criteria compliance se puede consultar a sys.configurations. Por ejemplo:

```
Select value from sys.configurations
Where name = ‘c2 audit mode’;
Go
Select value from sys.configurations
Where name = ‘common criteria compliance enabled’;
Go
```

Si el valor es igual a uno indica que se encuentra habilitada caso contrario el valor es cero.

En particular, si la opción de registro de los eventos de auditoria es SQL Trace debe consultarse a sys.traces para determinar si se encuentra activa una traza. Por ejemplo:

```
Select * from sys.traces
go
```

En la modalidad SQL audit, SQL Server provee un conjunto de vistas dinámicas y del sistema para facilitar la administración del registro de eventos de auditoría. El detalle de dichas vistas se adjunta en el Anexo XI.

1.5 Configuración y análisis de registros de eventos de auditoria en Oracle

Para elaborar el presente punto se utilizó la guía del estudiante del curso Oracle Database 11g: Security provisto por el fabricante del producto Oracle [6] y consultas en el sitio oficial de Oracle para la versión 12 c.

En versiones anteriores a 12c, Oracle proveía cinco tipos diferentes de registro de eventos de auditoria, a saber:

Básica: captura información parcial sobre el evento auditado. Registra el evento que ocurrió, cuando sucedió, el usuario que ejecutó el evento en cuestión y el cliente instalado en el equipo desde donde se origina el evento. Este tipo de auditoría se habilita con el comando AUDIT.

Basada en el valor: se registran los cambios en los datos, tiene en cuenta las sentencias de insert, delete o update. En este caso se registra la ocurrencia del evento y el valor que fue ingresado, actualizado o eliminado. Se implementa a través de triggers, con el comando CREATE TRIGGER. En particular, puede utilizarse este tipo de registro para capturar información adicional a la que la auditoria básica registra. Por ejemplo: la dirección ip del usuario que ejecuta un evento determinado.

Funcionalidad FGA (fine-grained auditing): este tipo es una extensión de la auditoria básica, permite focalizar sobre el tipo de evento que se quiere identificar, por ejemplo: registrar cuando se inserta un valor en una columna que supere un valor determinado. Este tipo de auditoria no requiere el uso de triggers y tiene un impacto en el rendimiento de la base de datos similar a la auditoría básica. Utiliza el paquete DBMS_FGA (en la versión 10g) y DBMS_AUDIT_MGMT (en la versión 11g r2). Se requiere que se asigne el permiso de ejecución sobre dicho paquete para la administración de las políticas. Se puede aplicar a las sentencias insert, delete, update y select. Además, utiliza el procedimiento DBMS_FGA.ADD_POLICY que acepta como argumento: nombre de la política, condición de auditoria, tipo de sentencia, columna y objeto a auditar, entre otros. Otros procedimientos que se emplean son: DBMS_FGA.ENABLE_POLICY (habilita la política), DBMS_FGA.DISABLE_POLICY (inhabilita la política) y DBMS_FGA.DROP_POLICY (elimina la política).

Sys Auditoría: Este tipo de auditoria permite monitorear las actividades de un administrador del sistema. Los usuarios que se conecten como SYS serán auditados y los registros de sus acciones serán escritos en un archivo del sistema operativo para evitar que sean borrados de la tabla aud$ de la base de datos. El parámetro de inicialización AUDIT_SYS_OPERATIONS se utiliza para activar y desactivar la auditoria de SYS.

Como complemento de estas soluciones y para proteger la información sensible recolectada, Oracle dispone del producto Oracle Audit Vault que se encarga de resguardar, centralizar y gestionar los registros de auditoria de distintas bases de datos y múltiples orígenes. [6]

En la versión Oracle 12c se incorporó una nueva forma de implementar y gestionar el registro de eventos de auditoría. Este nuevo

esquema permite agrupar varias políticas en una sola (de ahí el nombre de "unificada") permitiendo también crear políticas basadas en acciones (action-based) y condiciones (condition-based) si así fuera necesario. La implementación de este nuevo tipo de política es controlada por un usuario específico que es el dueño de las tablas de auditoria. Estas tablas son de sólo lectura, incluso para el propio usuario SYS. Por otro lado, todos los tipos de auditoria disponibles que puedan generarse son administrados por un único usuario y en una única tabla de seguimiento. Si se requiere dar acceso a otro usuario con nivel de administrador a los datos de auditoría (trail), se realiza a través de dos nuevos roles para tal fin, uno con privilegios únicamente de "viewer" y uno de "admin". [7]

Cuando se crea una nueva base de datos, por defecto la misma tiene el modo mixto de auditoria. Es decir el mecanismo tradicional, previo a la versión 12 c y las nuevas funcionalidades de la auditoria unificada. Oracle recomienda que se migre al modo de auditoria unificada una vez que el usuario se encuentre cómodo con esta nueva modalidad.

1.5.1 Configuración básica

El parámetro audit_trail define la ubicación donde los registros de eventos serán escritos, en Oracle 10 g el parámetro es estático y se encuentra deshabilitado por defecto, mientras que a partir de la versión 11 g r2 el mismo es dinámico y se encuentra configurado por defecto. En consecuencia, a partir de la versión 11 g r2 se empieza a registrar eventos sin la necesidad de reiniciar la base de datos. [8]

Los valores que pueden asignarse al parámetro son:

None : deshabilita la captura de registros de eventos.

DB : habilita la auditoria y guarda los registros en la base de datos.

DB, Extended: completa con mayor información las columnas sqlbind y sqltext de la tabla Sys.aud$.

XML : habilita la auditoria y escribe la totalidad de los registros de eventos en archivos en formato xml, por fuera de la base de datos.

XML, Extended: incorpora mayor información en los archivos de formato xml, incluyendo las columnas sqlbind y sqltext.

OS : habilita la auditoria y guarda los eventos en el registro de eventos del sistema operativo.

Para las opciones que escriben en archivos del sistema operativo, el directorio por defecto se determina con el parámetro audit_file_dest.

Cabe destacar que si los eventos se guardan en la base de datos pueden ser accedidos por SYSDBA, los usuarios con rol DBA y/o cualquier usuario con el privilegio any table. Por otro lado, si los registros se almacenan en archivos de formato xml o en el registro de eventos del sistema operativo, los mismos podrán ser accedidos por el administrador del equipo o cualquier usuario con permisos sobre el objeto.

La sintaxis para modificar audit_trail al valor DB, es:

ALTER SYSTEM SET audit_trail = "DB" SCOPE=SPFILE;

Para desactivar la auditoria se deba ejecutar el siguiente comando:

ALTER SYSTEM SET audit_trail = "NONE" SCOPE=SPFILE;

Para ejecutar este tipo de sentencias se require contar con el privilegio de ALTER SYSTEM.

Luego de configurar el parámetro audit_trail en un valor diferente a None se debe aplicar el comando audit. Este comando permite habilitar el registro de eventos de auditoria. La sintaxis del comando es la siguiente:

```
AUDIT
  { audit_operation_clause
  | audit_schema_object_clause
  | NETWORK
  } [ BY { SESSION | ACCESS } ]
    [ WHENEVER [ NOT ] SUCCESSFUL ]  ;
```

Donde

audit_operation_clause: activa la auditoria para una sentencia SQL concreta.

audit_schema_object_clause: activa la auditoria para un objeto concreto de la base de datos.

BY ACCESS: es la opción que se encuentra habilitada por defecto y registra cada acción que se realiza en forma separada.

BY SESSION: permite que se guarde un solo registro por sesión, por ejemplo si un usuario actualiza 100.000 registros en una tabla solo se guarda un único registro en la auditoría. [9]

WHENEVER SUCCESSFUL: activa la auditoria sólo para operaciones e instrucciones SQL que se completen con éxito.

WHENEVER NOT SUCCESSFUL: activa la auditoria sólo para operaciones e instrucciones SQL que generan error. Si esta cláusula se remueve completamente, se captura la totalidad de las acciones.

Se observa que a partir de la versión 11 g r2 algunas opciones de auditoria se encuentran habilitadas por defecto, las mismas son detalladas en el Anexo XII. Estas opciones tienen un impacto mínimo en el rendimiento de la base de datos. [8]

En el Anexo XIII se describen los comandos que se pueden auditar. [9]. Los mismos se pueden consultar en STMT_AUDIT_OPTION_MAP.

El usuario que activa la auditoria de objetos de un esquema, tiene que ser el propietario del objeto o disponer del privilegio de sistema AUDIT ANY.

Además, si el objeto que eligió para la auditoria se ubica en un directorio, incluso habiéndolo creado se necesita el privilegio de sistema AUDIT ANY.

El comando noaudit se utiliza para detener el registro de eventos de auditoria que se había activado previamente con la instrucción audit. Esta instrucción no influye en el parámetro audit_trail. Dicha sentencia debe tener la misma sintaxis que la instrucción audit que se desea desactivar.

La sintaxis del comando es la siguiente:

NOAUDIT

{ sql_statement_clause | *schema_object_clause* | *NETWORK}*

[WHENEVER [NOT] SUCCESSFUL] ;

Donde:

sql_statement_clause: detiene la auditoria de una sentencia SQL concreta.

schema_object_clause: detiene la auditoria para un objeto concreto de la base de datos.

WHENEVER SUCCESSFUL: detiene la auditoria sólo para operaciones e instrucciones SQL que se completen con éxito.

WHENEVER NOT SUCCESSFUL: detiene la auditoria sólo para operaciones e instrucciones SQL que generan error.

Para ejecutar el comando noaudit, el usuario necesita tener asignado el privilegio de sistema AUDIT SYSTEM. El usuario que desee detener la auditoria de objetos de un esquema, tiene que ser el propietario del objeto o disponer del privilegio de sistema AUDIT ANY. Además, si el objeto que eligió para la auditoria se ubica en un directorio, incluso habiéndolo creado dicho usuario, se requiere el privilegio de sistema AUDIT ANY.

1.5.2 Auditar a Sysdba y a los usuarios Sysoper

El Sysdba y los usuarios Sysoper tienen privilegios para iniciar y bajar la base de datos. Debido a que ellos pueden hacer cambios mientras la base de datos esta fuera de línea se deben registrar los eventos ejecutados por los mismos. La instancia captura los eventos de inicios de sesión para Sysdba y los usuarios Sysoper en forma automática pero no captura ningún otro evento que no este específicamente habilitado. Para habilitar el registro de eventos de estos usuarios se debe configurar el siguiente parámetro:

Audit_sys_operations = true

Los eventos se registrarán en el archivo que se configuró en el parámetro: audit_file_dest [6]

Para ejecutar esta sentencia se require contar con el privielgio de ALTER SYSTEM.

1.5.3 Auditoria unificada

La auditoria unificada se habilita por defecto. En caso de que no se encuentre habilitada se deberá configurar la librería pertinente. Para ello utilizar las siguientes sentencias:

cd $ORACLE_HOME/rdbms/lib

make -f ins_rdbms.mk uniaud_on ioracle

En esta modalidad todos los registros son escritos en un formato unificado y están disponibles a través de la vista Unified_audit_trail que se encuentra en el esquema AUDSYS. Los registros de eventos de auditoria se guardan en el tablespace SYSAUX por defecto. Se recomienda configurar un tablespace separado para este tipo de registros.

Con una política unificada se puede auditar: cuentas de usuarios, roles, privilegios, acciones sobre objetos (por ejemplo: eliminar una tabla), valores del contexto de una aplicación y actividades desde Oracle Database Real Application Security, Oracle Recovery Manager, Oracle Data Mining, Oracle Data Pump, Oracle SQL*Loader direct path events, Oracle Database Vault y Oracle Label Security.

Para configurar una política unificada de auditoria se utiliza la sentencia CREATE AUDIT POLICY. Si se quiere auditar valores del contexto de la aplicación y para habilitar la política se deberá emplear la sentencia AUDIT POLICY. Para ello se requiere del privilegio AUDIT SYSTEM o el rol AUDIT_ADMIN.

La sintaxis es la siguiente:

```
CREATE AUDIT POLICY policy_name
   { {privilege_audit_clause [action_audit_clause ] [role_audit_clause ]}
        | { action_audit_clause  [role_audit_clause ] }
             | { role_audit_clause }     }
          [WHEN audit_condition EVALUATE PER
        {STATEMENT|SESSION|INSTANCE}]
          [CONTAINER = {CURRENT | ALL}];
```

Donde

privilege_audit_clause se refiere a las opciones para auditar privilegios.

Para identificar los privilegios que se pueden auditar se puede consultar a la tabla SYSTEM_PRIVILEGE_MAP.

action_audit_clause y **standard_actions** describe las acciones que se registrarán.

role_audit_clause habilita la auditoria de los roles.

WHEN audit_condition EVALUATE PER habilita una función específica para una condición de una política unificada y evaluar la frecuencia.

CONTAINER se emplea para entornos de múltiples usuarios.

Por ejemplo:

Auditoria de un usuario con privilegio ANY

```
CREATE AUDIT POLICY hr_mgr_audit_pol
PRIVILEGES DROP ANY TABLE, DROP ANY CONTEXT, DROP
ANY INDEX, DROP ANY LIBRARY;
```

AUDIT POLICY hr_mgr_audit_pol BY HR_MGR;

Auditoria de un privilegio de sistema utilizando una condición

CREATE AUDIT POLICY os_users_priv_pol

PRIVILEGES SELECT ANY TABLE, CREATE LIBRARY

WHEN 'SYS_CONTEXT ("USERENV", "OS_USER") IN ("psmith", "jrawlins"')'

EVALUATE PER SESSION;

AUDIT POLICY os_users_priv_pol;

La auditoria unificada es propiedad de una nueva cuenta de usuario: AUDSYS. Con la nueva arquitectura existen una serie de colas “background queues”, dos por cliente, que reciben los registros de auditoria y los almacenan temporalmente, luego los datos son vaciados sobre la vista de solo lectura UNIFIED_AUDIT_TRAIL (propiedad del usuario SYS). Esta tarea la realiza un nuevo proceso llamado Gen0 (General Task Execution process) que continuamente, en un intervalo de 3 segundos, realiza la escritura sobre dicha vista. Como la vista es de sólo lectura, no hay posibilidad que el usuario SYS realice ninguna modificación, voluntaria o no, sobre la misma. Si por algún motivo se requiere vaciar la información manualmente, esto puede hacerse utilizando el paquete DBMS_AUDIT_MGMT como se muestra a continuación,

SQL>Exec SYS.DBMS_AUDIT_MGMT.Flush_Unified_Audit_Trail;

No debería haber ninguna necesidad de utilizar de manera explícita el paquete ya que el intervalo predeterminado de 3 segundos es suficiente para capturar toda la información de auditoria necesaria.

Como se mencionó anteriormente, la información de auditoria es capturada en primera instancia en colas de memoria. Cuando una cola se llena, su contenido es descargado (GEN0) y el cliente, por ejemplo RMAN, puede utilizar la otra cola para continuar almacenando su información de auditoria. Puesto que la captura de esta información de auditoria no necesariamente es un proceso síncrono y al ejecutarse el mismo en tal corto intervalo de tiempo, no tiene impacto negativo en el rendimiento de la base de datos. La memoria asignada por defecto para las colas es de 1 MB y puede ser configurada por el administrador con el parámetro UNIFIED_AUDIT_SGA_QUEUE_SIZE (el valor máximo permitido

es de 30 MB). La decisión para cambiar la memoria asignada debe hacerse en base a la cantidad estimada de información de auditoria. Para la mayoría de los sistemas, el valor por defecto de 1 MB debería ser suficiente.

Hay dos modos en los que operan las colas de auditoria: inmediato (Immediate) y encolado (Queued). Dependiendo del modo definido, la información de auditoria es descargada de manera inmediata o se vacía cada cierto intervalo. El modo por defecto es de encolamiento (queued) el cual hace que la información sea vaciada a disco sólo cuando las colas en memoria están completas. El modo de escritura inmediata tiene una manera de escribir la información mucho más intensa y, en consecuencia, podría llegar a afectar al rendimiento de manera significativa si la cantidad de información generada es alta. Se puede variar entre ambos modos de escritura utilizando el paquete DBMS_AUDIT_MGMT. El siguiente código habilita el modo de escritura IMMEDIATE modificando la configuración por defecto.

```
SQL>EXECUTE
DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_PROPERTY(-
DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED, -
DBMS_AUDIT_MGMT.AUDIT_TRAIL_WRITE_MODE, -
DBMS_AUDIT_MGMT.AUDIT_TRAIL_IMMEDIATE_WRITE);
```

Utilizando el mismo paquete, puede ser habilitado nuevamente el modo default Queued-Write.

Se acota que como la información de auditoria es generada y capturada primero en las colas, si ocurre un accidente dentro del intervalo de 3 segundos podría producirse la pérdida de los datos de ese período de tiempo. Pero teniendo en cuenta que ese intervalo es bastante corto, se supone que no debería haber una gran cantidad de datos perdidos, en caso de que existierá alguno. [10]

1.5.4 Visualización opciones de auditoria

En caso de utilizarse la modalidad básica para visualizar las opciones de auditoria que se seleccionaron, se pueden consultar las siguientes vistas:

Vista del diccionario de datos	Descripción

All_def_audit_opts	Opciones por defecto auditoria.
Dba_stmt_audit_opts	Opciones de auditoria establecidas.
Dba_priv_audit_opts	Opciones de auditoria de privilegio.
Dba_obj_audit_opts	Opciones de auditoria de objetos del esquema.

Se acota que las vistas muestran una columna por cada opción auditada. Por ejemplo, las opciones de auditoría de insert son mostradas en la columna INS. [6]

Adicionalmente, se puede consultar la configuración de los parámetros de la auditoria con la siguiente sentencia:

Show parameter audit

Con esta sentencia se puede conocer los valores de los parámetros audit_trail o audit_sys_operations.

Si se utiliza la modalidad FGA para consultar las opciones habilitadas, se debe ejecutar el comando: Desc DBA_AUDIT_POLICIES

Si se implementó la auditoria unificada, se puede consultar a la vista V$OPTION. Por ejemplo con la siguiente sentencia:

SELECT VALUE FROM V$OPTION WHERE PARAMETER = 'Unified Auditing';

En cuanto al detalle de las políticas habilitadas se puede consultar a la vista AUDIT_UNIFIED_POLICIES.

1.5.5 Análisis de los registros de eventos

Para la auditoria básica se puede consultar los registros de eventos de auditoria en las siguientes tablas:

DBA_AUDIT_TRAIL : totalidad de los registros de auditoria
DBA_AUDIT_STATEMENT: auditoria de cambios del sistema
DBA_AUDIT_SESSION : auditoria de sesiones
DBA_AUDIT_OBJECT : auditoria de objetos
V$XML_AUDIT_TRAIL : se completa si se emplea XML
DBA_AUDIT_EXISTS : errores de la auditoria

Si se utiliza la modalidad FGA se debe consultar a la vista DBA_FGA_AUDIT_TRAIL.

En el caso de que se emplee la auditoria unificada se debe consultar la vista Unified_audit_trail que se encuentra en el esquema AUDSYS.

En el Anexo XIV se adjunta el detalle de las tablas que guardan los registros de eventos para las distintas modalidades.

Capítulo II

2.1 Comparación entre los sistemas de gestión de base de datos relacional

2.1.1 Configuración de registros de eventos de auditoria

Con el fin realizar una comparación entre los diferentes mecanismos que utilizan los sistemas de gestión de base de datos relacional para la configuración del registro de eventos de auditoria se elaboró un cuadro comparativo que incluye las siguientes columnas:

Sistemas de gestión de base de datos relacional: denominación del producto comercial específico.

Script de instalación: informa el nombre del script que se requiere para contar con la funcionalidad del registro de eventos de auditoria. En caso de que dicha funcionalidad se encuentre incluída en el producto por defecto se completa con N/A, que significa no aplica.

Privilegios para ejecutar script de instalación: indica los tipos de permisos o privilegios que requiere el usuario para ejecutar el script de instalación de la funcionalidad del registro de eventos de auditoria.

Comandos de configuración: se señalan los comandos que se emplean para la configuración del registro de eventos de auditoria.

Privilegios para configurar la auditoria: indica los tipos de permisos o privilegios que requiere el usuario para ejecutar los comandos de configuración.

Nivel de auditoria: se refiere a los distintos niveles o alcances en el sistema de gestión de base de datos relacional donde se aplica la funcionalidad del registro de eventos.

Configuración en línea: Se completa con NO cuando se requiere reiniciar el servidor para que se habilite la funcionalidad del registro de eventos y con SI cuando el registro de eventos se habilita inmediatamente después de la configuración pertinente.

Repositorio de eventos: informa los almacenamientos físicos donde se guardan los registros de eventos de auditoria. Por ejemplo: tablas propias

del sistema de gestión de base de datos relacional, tablas definidas por el usuario, archivos o el registro de eventos del sistema operativo.

Gestión de almacenamiento y depuración de registros de eventos: da cuenta del mecanismo que se emplea para el almacenamiento y depuración de los registros de eventos. Algunos se realizan a través de procedimientos almacenados, tablas o parámetros propios del sistema de gestión de base de datos relacional y en algunos casos se requiere la implementación de tareas operativas.

Posibilidad de agregar registros: se refiere a la posibilidad de agregar eventos personalizados por el usuario. En caso de que sea factible se completa con la palabra SI y entre paréntesis se indica el procedimiento almacenado que brinda esta funcionalidad. Si no se puede incorporar eventos se integra la columna con la palabra NO.

Consulta de opciones de auditorias habilitadas: describe las tablas, los procedimientos almacenados o los comandos que se pueden consultar o ejecutar para identificar las opciones de auditoria que se encuentran habilitadas.

En el Anexo XVI se presenta un cuadro con los distintos tipos de configuraciones que se aplican a los sistemas de gestión de base de datos relacional.

En resumen, como resultado de la comparación se observa:

- Los sistemas de gestión de base de datos relacional SQL Server y Oracle han incorporado nuevas funcionalidades en el transcurso del tiempo y presentan varias opciones para la configuración de los registros de eventos de auditoria en comparación a SAP ASE y Teradata. Estos últimos solo disponen de una única variante para dicha funcionalidad. En consecuencia, podemos decir que SQL Server y Oracle son mas flexibles en cuanto a la configuración del registro de eventos.
- La funcionalidad de la configuración del registro de eventos de auditoria requiere la instalación de un script para SAP ASE, SQL Server con la opción Common Criteria Compliance y Oracle con la opciones Funcionalidad FGA y auditoria unificada. En el resto de los casos la funcionalidad en cuestión se encuentra disponible por defecto. Ante lo expuesto, se considera que la

necesidad de instalar la funcionalidad de registro de eventos aumenta las tareas operativas al momento de la configuración correspondiente.

- Cada sistema de gestión de base de datos relacional tiene sus propios comandos para habilitar el registro de eventos y sus determinados requerimientos para los privilegios del usuario que ejecuta los comandos en cuestión. Esta característica implica que se requiere un tratamiento diferente para cada uno de los sistemas de gestión de base de datos relacional. Dicha situación incrementa las tareas operativas de los administradores de las bases de datos y requiere de conocimientos técnicos específicos de cada sistema de gestión de base de datos relacional.
- En cuanto a los niveles en los que se puede aplicar el registro de eventos en los sistemas de gestión de base de datos relacional, Teradata tiene un enfoque únicamente por usuario. Los otros productos presentan mas opciones, tales como alcanzar el registro de eventos a nivel de servidor, base de datos y sentencias, entre otros. Esta particularidad dificulta la aplicación de un criterio homogéneo para el registro de eventos en todos los productos.
- Solo SQL Server requiere reinicio del servidor para que se active el registro de los eventos de auditoria, cuando se seleccionan las opciones C2, Common Criteria Compliance, SQL Trace y SQL Audit. Esta característica implica que la habilitación del registro de eventos de auditoria sea una tarea coordinada para garantizar la disponibilidad del servicio. Para los otros sistemas de gestión de base de datos relacional al configurar el registro de eventos se activa dicha funcionalidad sin otro requisito adicional, de tal forma de no comprometer la disponibilidad del servicio.
- En relación al repositorio de eventos de auditoria, Oracle y SQL Server brindan mayores opciones, a saber: archivos externos, tablas predefinidas, tablas definidas por usuarios y registro de eventos del sistema operativo. Por otro lado, SAP ASE y Teradata guardan los eventos en tablas de estructuras predefinidas. Para estos dos últimos casos, se debe tener en cuenta que un usuario con privilegios de administración podría eliminar los datos de auditoria, en consecuencia se deberían implementar controles específicos para detectar esta situación. En particular, SQL Server puede generar

archivos de extensión trc que tienen un formato propietario de Microsoft y requiere de herramientas específicas para su consulta.

- La gestión de almacenamiento y depuración de los registros de eventos puede automatizarse a través del empleo de procedimientos almacenados, tablas predefinidas o configuración de parámetros en SAP ASE, Teradata y SQL Server con sus opciones de SQL Trace y SQL Audit. En particular, Oracle con la opción de auditoria unificada solo cuenta con un procedimiento almacenado para liberar las colas donde se encuentran los eventos de auditoria y en el resto de las opciones requiere el diseño e implementación de tareas operativas para brindar esta funcionalidad. En los casos que se requieren implementar tareas operativas, se debe tener en cuenta que las mismas incrementan los costos y requieren tareas de monitoreo para garantizar su correcto funcionamiento.
- La posibilidad de agregar registros a los eventos de auditoria se encuentra disponible únicamente en SAP ASE y SQL Server en sus opciones SQL Trace, triggers y SQL Audit. Dicha característica ocasiona que se tengan que definir los procedimientos pertinentes para autorizar la incorporación de eventos de auditoria.
- Todos los sistemas de gestión de base de datos relacional cuentan con tablas, vistas o comandos que permiten consultar las opciones de auditorias habilitadas lo que permite verificar que se encuentren habilitadas las opciones correspondientes.

Adicionalmente a lo expuesto, se observa:

- La configuración y habilitación de registros de eventos de auditoria implican un consumo del 10 al 15 % del rendimiento de los sistemas de gestión de base de datos relacional, según informan los fabricantes de los productos comerciales.
- Las auditorias nativas no tienen costos monetarios adicionales en los productos empresariales.
- La gestión del almacenamiento y depuración de registros de eventos implica considerar costos relativos a los medios de almacenamiento y costos operativos.

2.1.2 Análisis de registros de eventos de auditoria

Con el fin realizar una comparación entre las distintas modalidades que ofrecen los sistemas de gestión de base de datos relacional para el análisis de los registros de eventos de auditoria se confeccionó un cuadro comparativo que cuenta con las siguientes columnas:

Sistemas de gestión de base de datos relacional: denominación del producto comercial específico.

Mecanismo para el análisis de eventos: se refiere a la modalidad que se emplea para efectuar el análisis de los registros de eventos de auditoria.

Privilegios: indica los privilegios o permisos que requiere el usuario para realizar el análisis de los registros de eventos de auditoria.

Repositorio de eventos: describe el repositorio físico que contiene los registros de eventos de auditoria.

¿Quién?: en este punto se brinda información para poder indentificar quien ejecutó el evento registrado. Se incluyen dos columnas, la primera con la descripción y la segunda con el nombre técnico del campo del repositorio que contiene los eventos

¿Cuándo?: informa que datos se deben consultar para identificar cuando se ejecutó el evento. Se presentan dos columnas, una con la descripción y otra con el nombre técnico del campo del repositorio que contiene los eventos.

¿Cómo?: detalla la información a consultar para detectar con que herramienta o medio se llevo a cabo el evento registrado. Por ejemplo, a través de una aplicación determinada. Se presentan dos columnas, una con la descripción y otra con el nombre técnico del campo del repositorio que contiene los eventos.

¿Qué?: describe que datos se deben consultar para obtener el detalle del evento registrado. Se presentan dos columnas, una con la descripción o detalle y otra con el nombre técnico del campo del repositorio que contiene los eventos.

En el Anexo XVII se presenta el cuadro comparativo del análisis de los registros de eventos en los sistemas de gestión de base de datos relacional.

En resumen, como resultado de la comparación se observa:

- Con respecto a los privilegios necesarios para acceder y analizar los eventos registrados, SAP ASE requiere que se asigne al usuario el rol SSO. Este rol además de poder consultar los eventos registrados puede crear usuarios, cambiar claves, asignar permisos, entre otros. Esta característica ocasiona que el usuario que debe consultar los eventos dispone de mayores privilegios que los necesarios. Por otro lado, para los sistemas de gestión de base de datos relacional restantes es factible limitar los permisos solo a la consulta de los eventos de auditoria registrados.En consecuencia, SAP ASE observa limitaciones en el cumplimiento de la asignación del menor privilegio para los usuarios que realizan las tareas de análisis de eventos.
- Todos los registros de eventos de los sistemas de gestión de base de datos relacional brindan información con diferentes niveles de detalles sobre quien ejecutó el evento, cuando y que hizo. Con respecto a como se llevo a cabo el evento, en SAP ASE este tipo de información se encuentra en el contenido del campo extrainfo de la tabla sysaudits y Oracle solamente contiene este tipo de datos para la opción de auditoria unificada. En consecuencia, SAP ASE y Oracle observan limitaciones en la información suministrada relativa a como se ejecutó el evento.
- Los registros de eventos de Teradata, SQL Server y Oracle brindan información detallada sobre el usuario que ejecutó el evento, incluyen datos, tales como: el equipo cliente, dirección ip, usuario del sistema operativo, el cual puede ser diferente al usuario de la base de datos. Estas carácterísticas permiten realizar un análisis exhaustivo. En cuanto a SAP ASE solo brinda información sobre el usuario del propio sistema de gestión de base de datos relacional y su número de identificación interno. Ante lo expuesto SAP ASE observa limitaciones en cuento a la información del usuario que ejecutó el evento.
- Teradata es el que mayor información ofrece con respecto a cuando se ejecuta el evento. Brinda en detalle distintas fechas y horas relacionadas con el evento registrado.
- Los registros de eventos de SAP ASE, Teradata, SQL Server y Oracle cuentan con información detallada sobre que se hizo en el evento en cuestión. Por ejemplo: evento ejecutado, objeto y base de datos accedido, resultado de la operación. En particular, Teradata brinda información

adicional sobre el rendimiento técnico, tales como cantidad de accesos al cpu.

- Para realizar el análisis de eventos registrados se requiere de operadores especializados con conocimiento del uso de las herramientas pertinentes, de las estructuras de los repositorios que guardan los eventos registrados y la codificación utilizada para registrar los eventos. Para cada sistema de gestión de base de datos relacional se tiene que implementar un mecanismo de análisis diferente lo que implica tareas operativas puntuales para cada uno de ellos.

Adicionalmente, con el fin de presentar un ejemplo práctico se elaboró un cuadro en el cual se puede observar los datos que se registran en los sistemas de gestión de base de datos relacional para el evento de inicio de sesión. En el Anexo XVIII se presenta el cuadro comparativo correspondiente.

Al respecto se consideraron las siguientes características comunes:
Nombre del usuario del sistema de gestión de base de datos relacional: TOM
Nombre del usuario que inicia sesión a nivel de red independientemente al sistema de gestión de base de datos relacional: TOM_SO.
Dirección ip del cliente: 10.2.49.235
Nombre del host del cliente: DOMINIO DE RED\PC
Dirección ip del servidor donde reside el sistema de gestión de base de datos relacional: 10.0.5.16
Nombre del servidor donde reside el sistema de gestión de base de datos relacional: SERVIDOR_BD
Nombre del dominio de red: DOMINIO DE RED

Como resultado del análisis del evento de inicio de sesión, se puede observar:

- El evento es registrado de distinta forma en cada uno de los sistemas de gestión de base de datos relacional. Para identificar el inicio de sesión se debe aplicar los siguientes criterios de búsquedas en los repositorios de eventos:

Sistema de gestión de base de datos relacional	**Criterio de búsqueda**

SAP ASE	El campo event de la tabla sysaudits debe ser igual a 45
Teradata	El campo QueryText de la tabla DBQLogTbl debe ser igual HELP SESSION
SQL Server	El campo EventClass del archivo de extensión trc debe ser igual a Audit Login
Oracle	El campo Action del archivo de formato xml debe ser igual a 100

-En SAP ASE no es factible identificar el usuario que inicia sesión en la red, el cual puede ser diferente del usuario que accede al sistema de gestión de base de datos relacional. Para el resto de los sistemas es factible identificar el usuario que inicio sesión en la red y el usuario propio del sistema.

-SQL Server, Teradata, SAP Ase y Oracle brindan precisión al incluir milisegundos en la fecha y hora de ejecución del evento. En particular, Teradata ofrece mayores referencias del evento debido a que indica los horarios en que se inicio la sentencia y el tiempo de respuesta de la misma.

-Para el presente ejemplo, en SAP ASE, Teradata y SQL Server es factible conocer a través de que aplicación se realizó el inicio de sesión. En el caso de Oracle al aplicar una auditoria estándar y guardar los registros de eventos en archivos de formato xml no es posible identificar la aplicación empleada por el usuario.

Capítulo III

En el presente capítulo se desarrolla la especificación del requerimiento, plan de trabajo e informe de situación actual para la configuración y el análisis de los registros de eventos de auditoría de los productos comerciales: Oracle 11 g r2, SAP ASE 16 SP 01, SQL Server 12 y Teradata 13.10 en una organización específica.

Con respecto a la organización, en el momento de iniciar el proyecto no se disponía de las configuraciones pertinentes para SQL Server 12, Teradata 13.10 y Oracle 11 g r2. Mientras que para SAP ASE 16 SP01 el registro de eventos de auditoría se encontraba configurado pero se observaban inconvenientes en el proceso de almacenamiento y depuración.

En cuanto al análisis del contenido de los eventos registrados no se efectuaba ninguna tarea y no se contaba con una herramienta específica para este fin.

Por otro lado, en cuanto a las áreas que intervienen en el proyecto, se acota lo siguiente:

- El área de seguridad informática es independiente del sector de infraestructura y es la responsable de definir los requerimientos de seguridad a aplicar a los componentes de la infraestructura y controlar el cumplimiento de los requisitos de seguridad.
- El sector de infraestructura cuenta con áreas que brindan diferentes servicios. Los sectores que participarán en el proyecto son el área encargada de la administración de la base de datos y el sector responsable de la administración del sistema operativo del servidor en el que reside la base de datos.

Adicionalmente, se destaca que el sector de auditoria en su informe de evaluación del control de acceso lógico a los datos observó los siguientes riesgos:

- usuarios de altos privilegios que pueden acceder a los datos por fuera de las aplicaciones y recomendó la habilitación de los registros de eventos en los sistemas de gestión de base de datos relacional y el monitoreo de las actividades de los usuarios de altos privilegios.

- usuarios de los sistemas de gestión de base de datos relacional que no ingresan a los mismos por mas de 90 días y recomendó que se realicen revisiones y depuraciones de usuarios para garantizar que solo tienen acceso los usuarios que lo requieran.

El proyecto es líderado por el área de seguridad informática.

3.1 Especificaciones del requerimiento

3.1.1 Objetivos

La presente especificación de requerimiento describe los requerimientos y las limitaciones para la configuración y el análisis de los registros de eventos de auditoría de los productos comerciales: Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10.

Los objetivos que se identifican son los siguientes:

- Configurar el registro de eventos de auditoría en Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10.
- Definir tareas de análisis del contenido de los registros de eventos de auditoría en Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10.

3.1.2 Participantes

Las siguientes personas han participado en las actividades de especificación de requerimientos:

Líder de proyecto
Administrador de Oracle 11 g r2
Administrador de SQL Server 12
Administrador de SAP ASE 16 SP01
Administrador de Teradata 13.10
Analista senior de seguridad Informática senior (dos)
Administador de los servidores donde residen los sistemas de gestión de base relacional (dos)

3.1.3 Situación actual

A continuación, se detalla el estado actual de cada sistema de gestión de base de datos relacional:

- Oracle 11 g r2, SQL Server 12 y Teradata 13.10: no cuentan con la configuración del registro de eventos de auditoria habilitada.
- SAP ASE 16.0 SP01: dispone de la configuración de registro de eventos y el almacenamiento y la depuración de eventos se realiza en forma manual diariamente.
- Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10: no tienen asociadas tareas de análisis de los registros de eventos de auditoria.

3.1.4 Problemas actuales

La siguiente es una lista de los problemas identificados durante los relevamientos y el análisis preliminar de estos sobre los requerimientos:

- El personal de seguridad informática necesita adquirir conocimientos técnicos y particulares relativos a la configuración y el análisis del registro de eventos de cada sistema de gestión de base de datos relacional.
- Los sectores de infraestructura solicitaron que la implementación de la configuración del registro de eventos de auditoria no impacte en mas de un 10 % en el rendimiento del sistema de gestión de base de datos relacional.
- Garantizar que los responsables de administrar las bases de datos no puedan modificar o eliminar los registros de eventos de auditoria.

3.1.5 Objetivos y Resultados Esperados

Los resultados esperados, una vez obtenido los productos del presente requerimiento, son:

- Implementar en el entorno productivo la configuración del registro de los eventos relevantes en Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10. Dichos eventos, al menos, deben incluir la totalidad de las acciones de los administradores de las bases de datos y los inicios de sesión exitosos y fallidos de la totalidad de los usuarios.
- El impacto de la implementación debe tener un efecto menor o igual al 10% en el rendimiento del servidor.

- Definir tareas de análisis de los registros de eventos de auditoria Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10.
- Implementar medidas de protección de la integridad de los registros de eventos de auditoria para SAP ASE 16.0 SP01 y Teradata 13.10.

3.1.6 Alternativas

Se presentan a continuación las opciones consideradas por cada sistema de gestión de base de datos relacional para la configuración del registro de eventos de auditoria:

Oracle 11 g r2

Alternativa 1: Habilitar la funcionalidad básica

Alternativa 2: Habilitar la funcionalidad para auditar a Sysdba y a los usuarios Sysoper

Alternativa 3: Habilitar la funcionalidad FGA

Análisis Comparativo

La siguiente tabla presenta la comparación entre las alternativas técnicas posibles en Oracle 11 g r2.

Criterio	Alternativas		
	1	2	3
Dificultad técnica de implementación	**Medio Alto** Requiere de ejecución de varios comandos	**Medio** Requiere de ejecución de un comando	**Alto** Requiere de ejecución de un script, definición de políticas particulares para registrar eventos de insert, delete y update
Impacto en el servidor	**Medio** La definición discrecional de los eventos a auditar pemite gestionar el impacto en el servicio	**Medio bajo** El impacto en el servicio es medio bajo porque la cantidad de eventos para este tipo de usuarios no es significativo	**Medio Alto** De acuerdo a la cantidad de políticas se puede observar un impacto medio alto en el servicio
Integridad de los registros de eventos	**Si** Se puede configurar que los archivos de eventos solo puedan ser accedidos por personal autorizado de Seguridad Informática	**Si** Se puede configurar que los archivos de eventos solo puedan ser accedidos por personal autorizado de Seguridad Informática	**No** Los datos capturados por las políticas son guardados en la tabla DBA_FGA_AUDIT_TRAIL. Dicha tabla puede ser modificada y eliminada por usuarios con privilegios de admistración de base de datos
Dificultad de análisis de eventos	**Medio Alto** La definición de los eventos a registrar previamente facilitan el análisis posterior	**Medio** Los eventos registrados correponden solo a SYSDBA y a usuarios SYSr lo que facilita el análisis	**Medio Alto** Los eventos a analizar son los que se definió en la configuración de las políticas. La ausencia de eventos adicionales o propios de Oracle facilitan el análisis

Se decidió implementar las **alternativas 1** y **2** correspondientes a las funcionalidades básica y auditar a Sysdba y a los usuarios Sysoper porque permiten definir los eventos a registrar, mas allá de los insert, delete y update que propone la funcionalidad FGA. Asimismo, definir los eventos a registrar previamente garantiza que el servicio no tendrá un alto impacto y el análisis de los eventos se facilita. Además, los eventos se guardarán en archivos de formato xml externos al sistema de gestión de base de datos relacional, de esta forma el administrador de base de datos no tendrá acceso a los mismos. Se descartó la funcionalidad FGA debido a la complejidad de su gestión. Además, el administrador de la base de datos podría modificar o eliminar los registros de eventos y solo permite registrar eventos de insert, delete y update.

Por otro lado, se acordó en primera instancia no habilitar el registro de eventos de select, insert y update debido a que no se pueden aplicar únicamente a los administradores de base de datos y en caso de implementarse se generarían un gran volumen de información. En forma paulatina y a medida que se clasifiquen los activos críticos de la información se habilitarán los registros para estos objetos.

Además, para las alternativas seleccionadas se requiere implementar procedimientos operativos para la gestión de almacenamiento y depuración de registros de eventos de auditoria.

En cuanto al análisis de los eventos se utilizarán scripts generados desde la línea de comandos para extraer los datos requeridos de los archivos en formato xml.

Adicionalmente, se requiere realizar mediciones para evaluar el impacto en el servidor cuando se habilite el registro de eventos y efectuar pruebas en el entorno de homologación antes de implementar el registro de eventos en el entorno productivo.

SQL Server 12

Alternativa 1: Habilitar la funcionalidad C2

Alternativa 2: Habilitar la funcionalidad Common Criteria Compliance

Alternativa 3: Habilitar la funcionalidad Trigger

Alternativa 4: Habilitar la funcionalidad SQL Trace

Alternativa 5: Habilitar la funcionalidad SQL Audit

Análisis Comparativo

La siguiente tabla presenta la comparación entre las distintas alternativas técnicas posibles en SQL Server 12.

Criterio	Alternativas				
	1	2	3	4	5
Dificultad técnica de implementación	**BAJO** Requiere de ejecución de un comando	**MEDIO ALTO** Requiere de ejecución de pocos comandos	**ALTO** Requiere la configuración de triggers específicos	**ALTO** Requiere la configuración de un script con los eventos a auditar, filtros a aplicar y definición de archivos de trazas	**ALTO** Requiere la configuración de sql audit a nivel de servidor y base de datos
Impacto en el servidor	**ALTO** Tiene un alto impacto generando inconvenientes en la disponibilidad del servicio	**ALTO** Tiene un alto impacto generando inconvenientes en la disponibilidad del servicio	**MEDIO ALTO** De acuerdo a la cantidad y anidamiento de los triggers se puede observar un alto impacto en el servicio	**MEDIO** La definición discrecional de los eventos a auditar y los filtros pertinentes pemiten gestionar el impacto en el servicio	**MEDIO** La definición discrecional de los sql audit pemiten gestionar el impacto en el servicio
Integridad de los registros de eventos	**SI** Se puede configurar que los archivos de eventos solo puedan ser accedidos por personal autorizado de Seguridad Informática	**SI** Se puede configurar que los archivos de eventos solo puedan ser accedidos por personal autorizado de Seguridad Informática	**NO** Los datos capturados por los triggers son guardados en tablas que pueden ser modificadas y eliminadas por usuarios con privilegios de admistración de base de datos	**SI** Se puede configurar que los archivos de eventos solo puedan ser accedidos por personal autorizado de Seguridad Informática	**SI** Se puede configurar que los archivos de eventos solo puedan ser accedidos por personal autorizado de Seguridad Informática
Dificultad de	**ALTO** Los eventos	**ALTO** Los eventos	**MEDIO** Los eventos a	**MEDIO ALTO** La definición	**MEDIO ALTO**

análisis de eventos	propios del SQL Server que se registran no pueden ser filtrados y dificultan el análisis	propios del SQL Server que se registran no pueden ser filtrados y dificultan el análisis	analizar son los que se definieron en la configuración de los triggers. La ausencia de eventos adicionales o propios del SQL Server facilita el análisis.	de los eventos a registrar previamente facilita el análisis posterior	La definición de los sql audit a registrar previa-mente facilita el análisis posterior.

Se decidió implementar la **alternartiva 4** correspondiente a la funcionalidad **SQL Trace** porque al definir los eventos a registrar previamente se garantiza que el servicio no tendrá un alto impacto y el análisis de los eventos se facilita. Además, al generar archivos de trazas externos al sistema de gestión de base de datos relacional se protege a los datos de posibles modificaciones o eliminaciones por parte de los administradores de base de datos. Se descarto la opción de SQL Audit porque la tarea de configurar a nivel de base de datos se debe realizar por cada una de ellas lo que lleva mayor tiempo si se tiene una gran cantidad de bases de datos. En cambio, con la opción SQL Trace se genera un script con todas las definiciones lo que simplifica la tarea de implementación.

Debido a que la alternativa elegida dispone de la funcionalidad de agregar eventos a los registros de auditoria se requiere implementar mecanismos de control adicionales para el tratamiento de esta excepción.

En cuanto al análisis de los eventos se utilizará la herramienta SQL Profiler para visualizar el contenido de los archivos trc.

Adicionalmente, se requiere realizar mediciones para evaluar el impacto en el servidor cuando se habilite el registro de eventos y efectuar pruebas en el entorno de homologación antes de implementar el registro de eventos en el entorno productivo.

SAP ASE 16.0 SP01

Alternativa única: Habilitar la funcionalidad de sybsecurity y tablas sysaudtis.

Análisis de la alternativa

La tabla siguiente presenta el análisis de la única alternativa que presenta SAP ASE.

Criterio	Alternativa
Dificultad técnica de implementación	**Alto** Requiere de ejecución de un script de instalación de la funcionalidad, definición de políticas particulares para registrar eventos y configuración de procedimientos almacenados para el almacenamiento y depuración de los eventos.
Impacto en el servidor	**Medio** La definición discrecional de los eventos a auditar pemiten gestionar el impacto en el servicio.
Integridad de los registros de eventos	**No** Los datos capturados son guardados en las tablas sysaudits que pueden ser modificados o eliminados por usuarios con privilegios de administración de base de datos.
Dificultad de análisis de eventos	**Medio Alto** La definición de los eventos a registrar previamente facilita el análisis posterior

En SAP ASE solo está disponible una única alternativa para implementar el registro de eventos de auditoria. En particular, los datos capturados son guardados en las tablas sysaudits que pueden ser modificados o eliminados por usuarios con privilegios de admistración de base de datos. Esta limitación implica que se deban definir procedimientos de controles compensatorios.

Debido a que la alternativa elegida dispone de la funcionalidad de agregar eventos a los registros de auditoria se requiere implementar mecanismos de tratamiento de esta excepción.

En cuanto al análisis de los eventos se utilizará la ejecución de sentencias select en las tablas sysaudits de la base de datos Sybsecurity. El usuario que realice las consultas requiere que se le asigne el rol SSO. Al respecto, este rol cuenta con mayores privilegios, tales como: habilitar o deshabilitar el registro de eventos, crear usuarios y cambiar claves de usuarios, entre otros.

Adicionalmente, se requiere realizar mediciones para evaluar el impacto en el servidor cuando se habilite el registro de eventos y efectuar pruebas en el entorno de homologación antes de implementar el registro de eventos en el entorno productivo.

Teradata 13.10

Alternativa única: Habilitar la funcionalidad de DBQL

Análisis de la alternativa

La tabla siguiente presenta el análisis de la única alternativa que presenta Teradata.

Criterio	Alternativa
Dificultad técnica de implementación	**Medio Alto** Requiere de la definición de reglas particulares para registrar eventos y configuración de tablas temporales e históricas para el almacenamiento y depuración de los eventos.
Impacto en el servidor	**Medio** La definición discrecional de los eventos a auditar pemiten gestionar el impacto en el servicio.
Integridad de los registros de eventos	**SI** Los datos capturados son guardados en las tablas DBQL que pueden ser modificados o eliminados por usuarios con privilegios de admistración de base de datos.
Dificultad de análisis de eventos	**Medio Alto** La definición de los eventos a registrar previamente facilita el análisis posterior.

En Teradata solo está disponible una única alternativa para implementar el registro de eventos de auditoria. En particular, los datos capturados son guardados en las tablas de DBQL que pueden ser modificados o eliminados por usuarios con privilegios de admistración de la base de datos. Esta limitación implica que se deban definir procedimientos de controles compensatorios.

Por otro lado, se identificó que no es factible registrar únicamente los inicios de sesión de todos los usuarios. Teradata captura la totalidad de eventos para un usuario y no se puede registrar uno en particular. Para

Teradata solo se registrarán las acciones de los usuarios con privilegios de admistración de base de datos.

En cuanto al análisis de los eventos se utilizará la ejecución de sentencias select en las tablas de la DBQL.

Adicionalmente, se requiere realizar mediciones para evaluar el impacto en el servidor cuando se habilite el registro de eventos y efectuar pruebas en el entorno de homologación antes de implementar el registro de eventos en el entorno productivo.

3.1.7 Descripción general de los requerimientos

Se espera que se lleve a cabo:

- La configuración del registro de eventos de auditoría en Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10.
- La definición de los procedimientos de análisis del contenido de los registros de eventos de auditoría en Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10.

3.1.8 Lista de los requerimientos

A continuación, se describen los requerimientos definidos durante las reuniones de extracción de requerimientos y elaborados en el análisis preliminar.

Nro	Requerimiento
1.	Configurar el registro de eventos de auditoria en Oracle 11 g r2 con la modalidad básica y el registro de Sysdba y de los usuarios Sysoper empleando archivos de formato xml para el resguardo de los eventos. Los eventos a registrar deben incluir la totalidad de las acciones de los administradores de las bases de datos (se exceptúan los eventos de select, insert, delete y update) y los inicios de sesión exitosos y fallidos de la totalidad de los usuarios. Definir los procedimientos operativos para el almacenamiento y depuración de los registros de eventos. Realizar las pruebas pertinentes en el entorno de homologación antes de la implementación en el entorno productivo.

	Efectuar mediciones del impacto en el servidor al implementar el registro de eventos de auditoria.
2.	Configurar el registro de eventos en SAP ASE 16.0 SP01 habilitando la sybsecurity con ocho tablas sysaudits. Los eventos a registrar deben incluir la totalidad de las acciones de los administradores de las bases de datos y los inicios de sesión exitosos y fallidos de la totalidad de los usuarios. Definir el proceso automático para el almacenamiento y depuración de los registros de eventos. Definir el procedimiento de control para detectar posibles eliminaciones o modificaciones de registros de la sybsecurity. Definir el procedimiento de excepción para la incorporación de eventos de auditoria. Realizar las pruebas pertinentes en el entorno de homologación antes de la implementación en el entorno productivo. Efectuar mediciones del impacto en el servidor al implementar el registro de eventos de auditoria.
3.	Configurar el registro de eventos en SQL Server 12 con la modalidad SQL Trace. Los eventos a registrar deben incluir la totalidad de las acciones de los administradores de las bases de datos y los inicios de sesión exitosos y fallidos de la totalidad de los usuarios. Definir los procedimientos operativos para el almacenamiento y depuración de los registros de eventos. Definir el procedimiento de excepción para la incorporación de eventos de auditoria. Realizar las pruebas pertinentes en el entorno de homologación antes de la implementación en el entorno productivo. Efectuar mediciones del impacto en el servidor al implementar el registro de eventos de auditoria.
4.	Configurar el registro de eventos en Teradata 13.10 habilitando la funcionalidad de DBQL. Los eventos a registrar deben incluir la totalidad de las acciones de los administradores de las bases de

	datos. Definir los procedimientos operativos para el almacenamiento y depuración de los registros de eventos. Definir el procedimiento de control para detectar posibles eliminaciones o modificaciones de registros de la BDQL. Realizar las pruebas pertinentes en el entorno de homologación antes de la implementación en el entorno productivo. Efectuar mediciones del impacto en el servidor al implementar el registro de eventos de auditoria.
5.	Definir los procedimientos de análisis del contenido de los registros de eventos de auditoría en Oracle 11 g r2 guardados en archivos de formato xml.
6.	Definir los procedimientos de análisis del contenido de los registros de eventos de auditoría en SAP ASE 16.0 SP01 residentes en la base de datos sybsecurity.
7.	Definir los procedimientos de análisis del contenido de los registros de eventos de auditoría en SQL Server 12 residentes en los archivos de extensión trc.
8.	Definir los procedimientos de análisis del contenido de los registros de eventos de auditoría Teradata 13.10 residentes en las tablas de BDQL.

3.2 Plan de trabajo

3.2.1 Antecedentes del proyecto

Alcance y restricciones

El presente plan de trabajo tiene como alcance configurar el registro de eventos de auditoría y definir procedimientos de análisis de eventos en Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10.

Las restricciones identificadas son:

- Necesidad de conocimientos técnicos y particulares relativos a la configuración y análisis de registro de eventos de auditoria de los sistemas de gestión de base relacional.

- La configuración del registro de eventos de auditoria no debe impactar en mas de un 10 % en el rendimiento del sistema de gestión de base relacional.
- Los productos SAP ASE 16.0 SP01 y Teradata 13.10 solo cuentan con una única modalidad para la configuración del registro de eventos que condiciona la integridad de los eventos registrados debido a que los usuarios con privilegios de administración de base de datos podrían eliminar las pistas de auditoria.
- La funcionalidad de registro de eventos de Teradata 13.10 no permite que se registren únicamente los eventos de inicio de sesión de usuarios.
- En Oracle 11 g r2 no es factible habilitar el registro de eventos por usuario, en consecuencia se acordó en primera instancia no habilitar el registro de eventos de select, insert, delete y update para los usuarios con privilegios de administración. En forma paulatina y a medida que se clasifiquen los activos críticos de la información se habilitarán los registros para estos objetos.

Objetivo general

- Configurar del registro de eventos de auditoría en Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10. Los eventos a registrar deben incluir la totalidad de las acciones de los administradores de las bases de datos y los inicios de sesión exitosos y fallidos de la totalidad de los usuarios para SAP ASE 16.0 SP01 y SQL Server 12. En cuanto a Teradata 13.10, los eventos a registrar deben incluir la totalidad de las acciones de los administradores de las bases de datos, se excluye el registro de los inicios de sesión del resto de los usuarios. Con respecto a Oracle 11 g r2 los eventos a registrar corresponden a los inicios de sesión exitosos y fallidos de la totalidad de los usuarios y la totalidad de las acciones de los administradores de las bases de datos, exceptuando los eventos de select, insert, delete y update
- Definición de los procedimientos de análisis del contenido de los registros de eventos de auditoría en Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10.

Objetivos específicos

Para Oracle 11 g r2

- Configurar el registro de eventos de auditoria con la modalidad básica y el registro de Sysdba y de los usuarios Sysoper empleando archivos de formato xml para el resguardo de logs.
- Habilitar el registro de los inicios de sesión exitosos y fallidos de la totalidad de los usuarios y la totalidad de las acciones de los administradores de las bases de datos, exceptuando los eventos de select, insert, delete y update.
- Definir los procedimientos operativos para el almacenamiento y depuración de los registros de eventos.
- Realizar las pruebas pertinentes en el entorno de homologación antes de la implementación en el entorno productivo.
- Efectuar mediciones del impacto en el servidor al implementar el registro de eventos de auditoria.
- Definir los procedimientos de análisis del contenido de los registros de eventos de auditoría guardados en archivos de formato xml.

Para SAP ASE 16.0 SP01

- Configurar el registro de eventos habilitando la sybsecurity con ocho tablas sysaudits.
- Habilitar el registro de la totalidad de las acciones de los administradores de las bases de datos y los inicios de sesión exitosos y fallidos de la totalidad de los usuarios
- Definir el proceso automático para el almacenamiento y depuración de los registros de eventos.
- Definir el procedimiento de control para detectar posibles eliminaciones o modificaciones de registros de la sybsecurity.
- Definir el procedimiento de excepción para la incorporación de eventos de auditoria.
- Realizar las pruebas pertinentes en el entorno de homologación antes de la implementación en el entorno productivo.
- Efectuar mediciones del impacto en el servidor al implementar el registro de eventos de auditoria.

- Definir los procedimientos de análisis del contenido de los registros de eventos de auditoría residentes en las tablas sysaudits de la sybsecurity.

Para SQL Server 12

- Configurar el registro de eventos con la modalidad SQL Trace y habilitar el registro de la totalidad de las acciones de los administradores de las bases de datos y los inicios de sesión exitosos y fallidos de la totalidad de los usuarios.
- Definir los procedimientos operativos para el almacenamiento y depuración de los registros de eventos.
- Definir el procedimiento de excepción para la incorporación de eventos de auditoria.
- Realizar las pruebas pertinentes en el entorno de homologación antes de la implementación en el entorno productivo.
- Efectuar mediciones del impacto en el servidor al implementar el registro de eventos de auditoria.
- Definir los procedimientos de análisis del contenido de los registros de eventos de auditoría en SQL Server 12 residentes en los archivos de extensión trc.

Para Teradata 13.10

- Habilitar el registro de la totalidad de las acciones de los administradores de las bases de datos utilizando la funcionalidad de DBQL.
- Definir los procedimientos operativos para el almacenamiento y depuración de los registros de eventos.
- Definir el procedimiento de control para detectar posibles eliminaciones o modificaciones de tablas de DBQL.
- Realizar las pruebas pertinentes en el entorno de homologación antes de la implementación en el entorno productivo.
- Efectuar mediciones del impacto en el servidor al implementar el registro de eventos de auditoria.
- Definir los procedimientos de análisis del contenido de los registros de eventos de auditoría residentes en las tablas de BDQL.

3.2.2 Planeamiento global del proyecto

Productos entregables

- Procedimiento de configuración, almacenamiento y depuración de los registros de eventos de auditoria en Oracle 11 g r2 con la modalidad básica y el registro de Sysdba y de los usuarios Sysoper empleando archivos de formato xml.
- Procedimiento de configuración, almacenamiento y depuración de los registros de eventos en SAP ASE 16.0 SP01 habilitando la sybsecurity con ocho tablas sysaudits.
- Procedimiento de configuración, almacenamiento y depuración de los registros de eventos en SQL Server 12 con la modalidad SQL Trace.
- Procedimiento de configuración, almacenamiento y depuración de los registros de eventos en Teradata 13.10 habilitando la funcionalidad de DBQL.
- Procedimiento de análisis del contenido de los registros de eventos de auditoría en Oracle 11 g r2 residentes en los archivos de formato xml.
- Procedimiento de análisis del contenido de los registros de eventos de auditoría en SAP ASE 16.0 SP01 residentes en la sybsecurity.
- Procedimiento de análisis del contenido de los registros de eventos de auditoría en SQL Server 12 residentes en los archivos de extensión trc.
- Procedimiento de análisis del contenido de los registros de eventos de auditoría Teradata 13.10 residentes en las tablas de BDQL.
- Procedimiento de control para detectar posibles eliminaciones o modificaciones de tablas sysaudits de la sybsecurity de SAP ASE 16.0 SP01.
- Procedimiento de control para detectar posibles eliminaciones o modificaciones de tablas de DBQL de Teradata 13.10.
- Procedimiento de excepción para la incorporación de eventos de auditoria en SAP ASE 16.0 SP01.
- Procedimiento de excepción para la incorporación de eventos de auditoria en SQL Server 12.
- Informe de resultados de las pruebas realizadas en el ambiente de homologación antes de la implementación en producción del registro de los

eventos de auditoria de Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10

- Informe de las mediciones del impacto en los servidores al implementar el registro de eventos de auditoria de Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10
- Informe de situación actual al cierre del proyecto.

Fases a cumplimentar

Las siguientes fases se aplican para cada uno de los sistemas de gestión de base relacional: Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10

1. Capacitación en administración del sistema de gestión de base relacional y en particular en aspectos de seguridad informática del producto.
2. Identificación de los eventos a registrar, a saber la totalidad de las acciones de los administradores de las bases de datos y los inicios de sesión exitosos y fallidos de la totalidad de los usuarios. Con excepción para Teradata que no incluye los inicios de sesión de los usuarios y en Oracle que se excluyen los eventos de select, insert, delete y update.
3. Definición de los mecanismos de almacenamiento y depuración para los registros de eventos a implementar.
4. Homologación en el entorno pertinente de la configuración, almacenamiento y depuración de los registros de eventos de auditoria. En esta fase se incluye la verificación correspondiente de la identificación y análisis de los eventos correspondientes a las acciones de los administradores de las bases de datos y los inicios de sesión exitosos y fallidos de la totalidad de los usuarios. Con excepción para Teradata que no incluye los inicios de sesión de los usuarios y Oracle que se excluyen los eventos de select, insert, delete y update.
5. Elaboración de los procedimientos de configuración, almacenamiento, depuración y análisis de los registros de evento de auditoria.
6. Elaboración de los procedimientos de control compensatorio para SAP ASE y Teradata.

7. Elaboración de los procedimientos de excepción para SAP ASE y SQL Server.
8. Implementación en el entorno de producción de la configuración, almacenamiento, depuración y análisis de los registros de eventos. Esta fase incluye el seguimiento y ajustes pertinentes que correspondan.
9. Medición del impacto en los servidores al implementar el registro de eventos de auditoria
10. Cierre del proyecto.

3.2.3 Planeamiento detallado del proyecto
Definición de actividades y tareas

Para identificar a las actividades y las tareas se utiliza la letra A y el número de la actividad.

Actividad	Tarea
A1 Capacitar en la administración y aspectos de seguridad de los sistemas de gestión de base relacional Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10	• Asistir al curso de Oracle 11 g r2 • Asistir al curso de SAP ASE 16.0 SP01 • Asistir al curso de SQL Server 2012 • Asistir al curso de Teradata 13.10
A2 Identificar los eventos correspondientes a la totalidad de las acciones de los administradores de las bases de datos y los inicios de sesión exitosos y fallidos de los usuarios	• Identificar los eventos pertinentes para Oracle 11 g r2, exceptuando los eventos de select, insert, delete y update. • Identificar los eventos pertinentes SAP ASE 16.0 SP01 • Identificar los eventos pertinentes SQL Server 2012 • Identificar los eventos pertinentes para Teradata 13.10. En este caso únicamente los eventos de los administradores.
A3 Definir los mecanismos de	• Definir los mecanismos de

almacenamiento y depuración para los registros de eventos de auditoria	almacenamiento y depuración pertinentes para Oracle 11 g r2 • Definir los mecanismos de almacenamiento y depuración pertinentes para SAP ASE 16.0 SP01 • Definir los mecanismos de almacenamiento y depuración pertinentes para SQL Server 2012 • Definir los mecanismos de almacenamiento y depuración pertinentes para Teradata 13.10
A4 Homologar la configuración, los mecanismos de almacenamiento y depuración y el análisis de los registros de eventos de auditoria	• Homologar la configuración, los mecanismos de almacenamiento y depuración y el análisis de eventos pertinentes para Oracle 11 g r2 • Homologar la configuración, los mecanismos de almacenamiento y depuración y el análisis de eventos pertinentes para SAP ASE 16.0 SP01 • Homologar la configuración, los mecanismos de almacenamiento y depuración y el análisis de eventos pertinentes para SQL Server 2012 • Homologar la configuración, los mecanismos de almacenamiento y depuración y el análisis de eventos pertinentes para Teradata 13.10
A5 Elaborar los procedimientos de configuración, almacenamiento, depuración, análisis de los registros de evento de auditoria y los	• Elaborar los procedimientos pertinentes para Oracle 11 g r2 • Elaborar los procedimientos pertinentes para SAP ASE 16.0

procedimientos de control adicionales.	SP01 • Elaborar los procedimientos pertinentes para SQL Server 2012 • Elaborar los procedimientos pertinentes para Teradata 13.10
A6 Elaboración de los procedimientos de control adicionales para SAP ASE, Teradata y SQL Server	• Elaborar el procedimiento para detectar la eliminación o modificación de los registros de eventos en SAP ASE 16.0 SP01. • Elaborar el procedimiento para detectar la eliminación o modificación de los registros de eventos en Teradata 13.10 • Elaborar el procedimiento de excepción para agregar registros de auditoria en SAP ASE 16.0 SP01 Elaborar el procedimiento de excepción para agregar registros de auditoria en SQL Server 2012
A7 Implementar en el entorno productivo la configuración, almacenamiento, depuración y análisis de los registros de eventos de auditoria	• Implementar en el entorno productivo de Oracle 11 g r2 • Implementar en el entorno productivo de SAP ASE 16.0 SP01 • Implementar en el entorno productivo de SQL Server 2012 • Implementar en el entorno productivo de Teradata 13.10
A8 Medir el impacto en los servidores al implementar el registro de eventos de auditoria	• Medir el impacto en el servidor de Oracle 11 g r2 al configurar el registro de eventos de auditoria • Medir el impacto en el servidor de SAP ASE 16.0 SP01 al configurar el registro de eventos de auditoria

	• Medir el impacto en el servidor de SQL Server 2012 al configurar el registro de eventos de auditoria • Medir el impacto en el servidor de Teradata 13.10 al configurar el registro de eventos de auditoria Se debe tener en cuenta que para implementar en producción se requiere que el impacto no sea mayor al 10%
A9 Cierre del proyecto	• Elaborar un informe de situación actual al finalizar el proyecto.

Secuencia temporal de actividades

Para Oracle 11 g r2 se ejecutan en forma secuencial la tarea correspondiente de las actividades: A1, A2, A3, A4, A5 y A7. Para SAP ASE 16.0 SP01, SQL Server 2012 y Teradata 13.10 corresponden las tareas de las actividades A1, A2, A3, A4, A5, A6 y A7.

En cuanto a la tarea pertinente de la actividad A8 debe efectuarse en forma paralela a la tarea de homologación (A4) y a la de implementación en producción (A7) para todos los sistemas de gestión de base de datos relacional.

Al finalizar con un sistema de gestión de base relacional se continuará con el siguiente, el orden acordado es: Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 2012 y Teradata 13.10

Al concluir con todas las implementaciones en producción se ejecutará el cierre del proyecto (A9).

Recursos asociados a actividades

Los siguientes recursos asociados a las actividades A1, A2, A3, A4, A5, A6, A7 y A8 aplican a un sistema de gestión de base relacional.

Se acota que el cálculo financiero solamente considera la cantidad de horas requeridas por actividad.

Actividad	Recursos			
	Humanos	**Material**	**Técnicos**	**Financiero**
A1	2 Analistas Senior de Seguridad Informática 1 Líder de proyecto	No se requieren. La capacitación se realiza en instalaciones externas a la organización	No se requieren. La capacitación se realiza en instalaciones externas a la organización	Curso de 40 hs
A2	2 Analistas Senior de Seguridad Informática 1 Líder de proyecto 1aministrador de base de datos	Oficina de reuniones Escritorios de trabajo Impresora Papel	Acceso a internet Computadora Manuales técnicos Servidores del entorno de homologación	40 hs por cada Analista Senior de Seguridad Informática **Total**: 80 hs 8 h de Líder de proyecto **Total**: 8 hs 8 h por cada administrador de base de datos **Total:** 8 hs
A3	2 Analistas Senior de Seguridad Informática 1 líder de proyecto 1administrador de base de datos	Oficina de reuniones Escritorios de trabajo Impresora Papel	Acceso a internet Computadora Manuales técnicos Servidores del entorno de homologación	24 hs por cada Analista Senior de Seguridad Informática **Total**: 48 hs 4 hs de Líder de proyecto **Total**: 4 hs 8 hs por cada administrador de base de datos **Total:** 8 hs
A4	2 Analistas Senior de Seguridad Informática 1 Líder de proyecto 1administrador de base de	Oficina de reuniones Escritorios de trabajo Impresora Papel	Acceso a internet Computadora Manuales técnicos Servidores del entorno de homologación	40 hs por cada Analista Senior de Seguridad Informática **Total**: 80 hs 16 hs de Líder de proyecto

	datos 1 administrador de servidor			**Total**: 16 hs 24 hs por cada administrador de base de datos **Total:** 24 hs 16 hs por cada administrador de servidor **Total:** 16 hs
A5	2 Analistas Senior de Seguridad Informática 1 Líder de proyecto	Oficina de reuniones Escritorios de trabajo Impresora Papel	Acceso a internet Computadora Manuales técnicos	24 hs por cada Analista Senior de Seguridad Informática **Total**: 48 hs 8 hs de Líder de proyecto **Total**: 8 hs
A6	2 Analistas Senior de Seguridad Informática 1 Líder de proyecto	Oficina de reuniones Escritorios de trabajo Impresora Papel	Acceso a internet Computadora Manuales técnicos	16 hs por cada Analista Senior de Seguridad Informática **Total**: 32 hs 4 hs de Líder de proyecto **Total**: 4 hs
A7	2 Analistas Senior de Seguridad Informática 1 Líder de proyecto 1administrador de base de datos 1 administrador del servidor	Oficina de reuniones Escritorios de trabajo Impresora Papel	Acceso a internet Computadora Manuales técnicos Servidores del entorno homologación y productivo	40 hs por cada Analista Senior de Seguridad Informática **Total**: 80 hs 16 hs de Líder de proyecto **Total**: 16 hs 24 hs por cada administrador de base de datos **Total:** 24 hs 24 Hs por cada administrador de servidor **Total:** 24 hs
A8	2 Analistas Senior de	Oficina de reuniones	Acceso a internet	20 hs por cada Analista Senior

	Seguridad Informática 1 Líder de proyecto 1administrador de base de datos 1 administrador del servidor	Escritorios de trabajo Impresora Papel	Computadora Manuales técnicos Servidores del entorno homologación y productivo	de Seguridad Informática **Total**: 40 hs 5 hs de Líder de proyecto **Total**: 5 hs 10 hs por cada administrador de base de datos **Total:** 10 hs 20 hs por cada administrador de servidor **Total:** 20 hs
A9	1 Líder de proyecto	Escritorios de trabajo Impresora Papel	Acceso a internet Computadora	32 hs de Líder de proyecto **Total**: 32 hs

Costos del proyecto
Costos por fase

Los costos son expresados en horas.

Fase	Costo en horas por sistema de gestión de base de datos relacional	Costo total en horas del proyecto
A1	120	480
A2	96	384
A3	60	240
A4	136	544
A5	56	224
A6 (*)	36	108
A7	144	576
A8	75	300
A9	32	32

(*) Con respecto a la fase A6 solo se aplica a SAP ASE 16.0 SP01, SQL Server 2012 y Teradata 13.10.

Plan de Adquisiciones y contrataciones

El proyecto se realiza con personal y recursos materiales de la organización no se requieren adquisiciones ni contrataciones.

Costo total y duración total

El costo total estimado es de 2888 horas y la duración total es de aproximadamene 25 semanas (se incluyen 4 semanas de capacitación, una por cada sistema de gestión de base de datos relacional).

Criterios de calidad y análisis de riesgos
Identificación de riesgos

Los principales riesgos identificados son:

1. Desafectación de recursos humanos. Reasignación de nuevas tareas a los recursos humanos participantes del proyecto.
2. Los tiempos dedicados al proyecto no son los suficientes
3. Dificultad técnica en adquirir el conocimiento necesario para concretar los productos esperados.
4. Falta de herramientas técnicas, administrativas y operativas a utilizar.

3.3 Informe de situación final

Para confeccionar el siguiente informe se consultó el sitio de internet mencionado en la referencia [18]

Se efectuaron satisfactoriamente, en tiempo y forma los siguientes trabajos:

- configuración del registro de eventos de auditoría en Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10. Para todos los sistemas se logro que el impacto de la configuración no supere el 10% en los servidores involucrados en el entorno productivo vigente. En el Anexo XV se da cuenta de las opciones configuradas para los distintos sistemas de gestión de base de datos relacional.
- implementación de los procesos de almacenamiento y depuración de los registros de eventos en todos los sistemas de gestión de base de datos relacional con el fin de evitar pérdidas de eventos y disponer de los mismos para consultas futuras.
- definición de los controles pertinentes para detectar eliminaciones de pistas de auditoria en SAP ASE 16.0 SP01 y Teradata 13.10.

- definición de tratamiento de excepciones para agregar registros de eventos de auditoria en SAP ASE 16.0 SP01 y SQL Server 2012.
- definición de los procedimientos para el análisis de los eventos registrados en los sistemas de gestión de base de datos relacional. Los eventos en cuestión responden a la totalidad de las acciones de los administradores de las bases de datos y los inicios de sesión exitosos y fallidos de la totalidad de los usuarios para SAP ASE 16.0 SP01 y SQL Server 12. En cuanto a Teradata 13.10 solo se analizan las acciones de los administradores de las bases de datos y en Oracle 11 g r2 se exceptuaron los eventos de select, insert, delete y update de los administradores de la base de datos.

Dificultades encontradas

Durante la ejecución del proyecto se presentaron algunas dificultades técnicas que responden a las características propias de los sistemas de gestión de base de datos relacional, a saber:
- en Oracle 11 g r2 para la configuración implementada se observó en el directorio donde residen los archivos de eventos, tres tipos distintos de archivos:
1. archivos con el nombre del tipo xml_identificación del proceso, por ejemplo: ora_1136.xml. La identificación del proceso puede repetirse en distintos momentos, esto ocasiona que los datos de diferentes momentos se adjunten al archivo existente. Es decir que en un archivo xml se puede encontrar información de distintas fechas.
2. achivos con el nombre del tipo pmon_identificación del proceso, por ejemplo: pmon_5589.xml. Estos archivos contienen datos de los eventos 102 (LOGOFF BY CLEANUP). Este evento corresponde a inicios de sesión que no tienen su correspondiente cierre de sesión.
3. un archivo con el nombre Adx_instancia del servidor, por ejemplo: adx_serverprod.txt que constituye un índice de los archivos xml generados
4. Esta situación, incrementó la complejidad en las tareas de análisis debido a que los datos de un usuario para un día determinado deben buscarse en varios archivos.

- en SQL Server 2012 para la modalidad seleccionada correspondiente a SQL Trace fue necesario realizar un trabajo exhaustivo para filtrar los eventos que no eran relevantes. Dicha tarea prolongó el tiempo estimado en la fase de homologación. Este tiempo fue recuperado posteriormente porque otros sistemas necesitaron un menor tiempo de trabajo. Asimismo, en las tareas de análisis de los eventos se identificó que no se registran los valores de las variables involucradas en la sentencia. Por ejemplo, se puede interpretar la ejecución de una modificación de datos, pero no se puede detectar que valores fueron modificados. En consecuencia, se considera que el análisis de eventos para SQL Server 2012 es satisfactorio presentando limitaciones. La calificación de satisfactorio, es sobre una escala de: insatisfactorio, satisfactorio y muy satisfactorio.
- En SAP ASE 16.0 SP01 durante las tareas de análisis de eventos se identificó que no se registran las sentencias contenidas en los procedimientos almacenados, únicamente se registra la ejecución del procedimiento almacenado. En consecuencia, se considera que el análisis de eventos para SAP ASE 16.0 SP01 es satisfactorio presentando limitaciones. La calificación de satisfactorio, es sobre una escala de: insatisfactorio, satisfactorio y muy satisfactorio.
- En SAP ASE 16.0 SP01 y Teradata 13.10 la cantidad de eventos disponibles en línea fueron condicionados por la disponibilidad de espacio de disco de dichos sistemas.

Por otro lado, en cuanto a la capacitación para SAP ASE 16.0 SP01 y Teradata 13.10 fue necesario solicitar un curso a medida a los fabricantes porque no disponen de cursos abiertos a todo el público. Dicha situación ocasionó que se empiece a trabajar en la identificación de los eventos a registrar en forma previa a la capacitación.

Adicionalmente, en la fase de homologación para todos los sistemas de gestión de base relacional se detectó que algunas alteraciones en la forma habitual de trabajo podrían ocasionar que se generen una gran cantidad de eventos y en consecuencia se incremente el volumen de los registros. Por ejemplo, cuando en una sesión una clave de usuario caduca, se pueden generar una gran cantidad de inicios de sesión fallidos o si un administrador de base de datos utiliza todo el tiempo una herramienta de

monitoreo sobre el sistema se observan una numerosa cantidad de eventos que responden a consultas a tablas internas del sistema.

Asimismo, en relación al análisis de eventos se observó que el seguimiento detallado de las acciones ejecutadas por un administrador de base de datos requiere un tiempo considerable para su elaboración y para detectar los eventos críticos.

En particular para Oracle 11 g r2 no fue factible incorporar el registro de los eventos select, insert, delete y update porque no se finalizó el proceso de clasificación de activos críticos.

Relaciones con terceros

No se presentaron dificultades entre los tres sectores intervenientes. En algunas ocasiones fue necesario reprogramar reuniones debido a que los administradores de base de datos y/o administradores de los servidores estaban asignados a tareas urgentes relacionadas con la disponibilidad de los servicios que gestionan. Asimismo, fue factible cumplir con los plazos de tiempos preestablecidos.

Acciones futuras

Con el fin de mejorar el análisis de los registros de eventos, se recomienda:

- definir un criterio para detectar los eventos realizados por los administradores de base de datos que sean críticos y relevantes a la seguridad informática.
- evaluar la factibilidad de mejorar el proceso de análisis con el desarrollo de un aplicativo que facilite esta tarea.

Resumen del estado:

	SI	**NO**
Modificaciones al alcance		x
Retrasos		x
Incremento del riesgo		x
Sobrecoste		x

Insatisfacción del Cliente	x
Ampliaciones al contrato	x
Carencia de recursos	x
Conflictos interpersonales	x
Falta de formación y/o experiencia	x

Capítulo IV

En el presente capítulo se desarrolla la especificación del requerimiento, plan de trabajo e informe de situación actual para el proyecto de análisis de eventos de auditoria de los sistemas de gestión de base de datos relacional utilizando una herramienta específica en una organización determinada.

En dicha organización la información es gestionada a través de los sistemas de gestión de base de datos relacional Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10. En todos estos sistemas se encuentran configurada la funcionalidad del registro de eventos de auditoria y se efectúa periódicamente el análisis de los eventos capturados.

En cuanto a las áreas que intervienen en el proyecto, se acota lo siguiente:

El área de seguridad informática es independiente del sector de infraestructura y es la responsable de definir los requerimientos de seguridad a aplicar a los componentes de la infraestructura y controlar el cumplimiento de los requisitos de seguridad.

El sector de infraestructura cuenta con áreas que brindan diferentes servicios. Los sectores que participarán en el proyecto son el área encargada de la administración de la base de datos, sector responsable de los servidores donde residen los sistemas de gestión de la base de datos relacional y el departamento encargado de la administración de la red informática.

El proyecto es líderado por área de seguridad informática.

4.1 Especificaciones del requerimiento

4.1.1 Objetivos

La presente especificación de requerimiento describe los requerimientos y las limitaciones para la implementación del análisis de eventos de Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10 utilizando una herramienta específica para este fin.

Los objetivos que se identifican son los siguientes:

- Definir diez eventos críticos para la seguridad informática en los sistemas de gestión de base de datos relacional basados en los principales riesgos identificados.
- Analizar con la herramienta específica los diez eventos críticos definidos.
- Definir los procedimientos de análisis para los diez eventos críticos en cuestión.

4.1.2 Participantes

Las siguientes personas han participado en las actividades de especificación de requerimientos:

Líder de proyecto

Administrador de base de datos con conocimientos de Oracle, SQL Server, SAP ASE y Teradata

Administrador de los servidores donde residen los sistemas de gestión de base de datos relacional.

Analista senior de seguridad Informática (dos)

Administador de la herramienta de análisis de eventos

Administador de la red informática corporativa

4.1.3 Situación actual

Al iniciar el presente requerimiento la organización tiene habilitado el registro de eventos en los sistemas de gestión de base de datos relacional, con las siguientes características:

SAP ASE 16.0 SP01 y SQL Server 12: se registran la totalidad de las acciones de los administradores de base de datos y los inicios de sesión exitosos y fallidos de la totalidad de usuarios.

Oracle 11 g r2: registra la totalidad de los inicios de sesión exitosos y fallidos de la totalidad de usuarios y las acciones de los administradores de base de datos, exceptuando los eventos de select, insert, delete y update.

Teradata 13.10: registran la totalidad de las acciones de los administradores de base de datos.

Para todos los casos la implementación de la configuración del registro de eventos no ocasionó inconvenientes en la disponibiliad del

servicio. En ninguno de los sistemas se observó que la impementación tenga una carga en el rendimiento de cpu superior al 10 %.

Asimismo, se implementaron tareas regulares para el análisis de eventos de todos los sistemas de gestión de base de datos relacional. Al respecto, se observó lo siguiente:

- las actividades de análisis requieren mucho tiempo operativo y el uso de distintos aplicativos para su explotación.
- la elaboración de los reportes para el nivel gerencial deben ser confeccionados manualmente debido a la heterogeneidad de las fuentes de información.
- la detección de los eventos relevantes no es oportuna en el tiempo. Esta situación impedía tomar acciones para el tratamiento pertinente de los posibles incidentes de seguridad.
- en algunas ocasiones no era factible identificar la totalidad de los datos de los eventos. Por ejemplo: En SAP ASE no es factible identificar el usuario que inicia sesión en la red, el cual puede ser diferente del usuario que accede al sistema de gestión de base de datos relacional.
- en el caso de los procedimientos almacenados no se registra el detalle de las sentencias de su contenido, únicamente se registra el nombre del procedimiento y el evento de ejecución.

Ante lo expuesto, la organización decidió adquirir una herramienta específica para el análisis de eventos. El producto comercial responde al nombre: SecureSphere Database Activity Monitoring de Imperva versión 11.5

Se destaca como principales características de esta herramienta:

- Los eventos que captura de los distintos sistemas de gestión de base de datos relacional tienen el mismo formato. La herramienta es compatible con Oracle, Teradata, SAP ASE y SQL Server entre otras.
- Generación de alertas en tiempo real de los eventos configurados previamente. Incluye la posibilidad de bloquear la acción.
- Interfaz de fácil uso que permite visualizar, analizar y correlacionar eventos.
- Disponibilidad de informes predefinidos de nivel gerencial y operativo.
- Permite la separación de funciones a través de diferentes roles.

- Garantiza la integridad de los eventos capturados.
- Identifica patrones normales de acceso de los usuarios a la información, estableciendo una línea base de toda la actividad de los usuarios.

En el proceso de implementación, se acordó entre el sector de infraestructura y seguridad informática implementar la herramienta en modalidad fuera de línea con agentes locales en los servidores de las bases de datos. Este mecanismo copia y envia el tráfico de red que entra y sale del sistema de gestión de base de datos relacional a la herramienta para su procesamiento. Con respecto a los agentes locales, los mismos son instalados en cada servidor y tienen como funcionalidad enviar el tráfico local (el que no pasa por la red) a la herramienta específica.

En el proceso de puesta en producción de la herramienta, se observó lo siguiente:

-los agentes locales pueden superar el 10 % ante una gran cantidad de eventos (si son configurados para enviar la totalidad del tráfico sql) y ser deshabilitados por los administradores de servidores, lo que ocasionaría posibles pérdidas de eventos. En consecuencia, se requiere de un monitoreo sobre el estado de los agentes y tratamiento de las alertas detectadas.

- los cambios en la red pueden ocasionar pérdidas de eventos. Por ejemplo: si el ancho de banda del tráfico de red supera la capacidad de procesamiento de la herramienta o si se modifica la configuración del switches que envian el tráfico de la red a la herramienta. Para evitar estos inconvenientes, se necesita un monitoreo sobre la recepción de eventos de la herramienta.

- no se puede interpretar el contenido de ciertos eventos de algunos programas enlatados. En este caso solo se observan llamadas a funciones o procedimientos y no el detalle de las acciones particulares. Al respecto, fue factible identificar este tipo de eventos en el registro de eventos propio del sistema de gestión de base de datos relacional. Para solucionar este inconveniente se requiere instalar el agente local en el servidor y que el mismo transmita la totalidad de los eventos y no solo los eventos locales.

- se requiere proteger con caracteres o encubrir los datos sensibles que se encuentran en texto claro en la red, por ejemplo: claves de usuarios.

- si algún sistema de gestión de base de datos relacional utiliza el protocolo ssl con un cliente, es necesario realizar la configuración pertinente en la herramienta con los certificados digitales correspondientes.
- inconvenientes en la identificación de usuarios finales relacionados con autenticación integrada del sistema de gestión de base de datos relacional con un active directory. En este caso los usuarios son denominados como Hashed user.
- demoras en la visualización de datos debido a la sobrecarga del procesamiento interno de la herramienta por exceso de eventos recibidos. El incremento de eventos pueden ser resultantes de implementaciones erróneas de desarrollos, por ejemplo: una consulta que se ejecuta cada un segundo a una tabla.

En resumen, debido a la modalidad seleccionada para la implementación de la herramienta se podrían presentar pérdidas de eventos si los agentes locales no envían datos y/o el volumen de información enviado a la herramienta es superior a su capacidad de procesamiento. Además, no es factible bloquear las acciones. La herramienta tiene un carácter detectivo.

4.1.4 Problemas actuales

La siguiente es una lista de los problemas identificados durante los relevamientos y el análisis preliminar de estos sobre los requerimientos:
- Al momento de iniciar el proyecto no se encuentra finalizada la clasificación de los activos informáticos críticos. Esta situación impide que los controles se apliquen a los componentes críticos de los sistemas de gestión de base de datos relacional. Por ejemplo: detectar que se actualizan montos superiores a un valor en una tabla crítica o identificar intentos de consultas a datos confidenciales.
- Se requiere la colaboración de los sectores de infraestructura para monitorear el correcto funciomiento de la herramienta.

4.1.5 Objetivos y Resultados Esperados

Los resultados esperados, una vez obtenido los productos del presente requerimiento, son:

- Implementar procedimientos para el análisis de diez eventos críticos para la seguridad informática de los sistemas de gestión de base de datos relacional utilizando la herramienta de análisis específica. Los sistemas de gestión de base de datos relacional a considerar son: Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10.
- Profundizar los conocimientos en el uso de la herramienta en cuestión.

4.1.6 Alternativas

Luego de varias reuniones se definió una única alternativa con los diez eventos críticos a analizar con la herramienta específica. Dicha definición pretende dar respuesta a los siguientes riesgos identificados en la organización:

- acciones de usuarios de altos privilegios sobre los datos del entorno productivo por fuera de las aplicaciones (eventos 1, 2, 5 y 9).
- usuarios que tienen permisos de altos privilegios que no corresponde por las tareas laborales asignadas (evento 3).
- accesos de usuarios no autorizados (eventos 4 y 6).
- clave del usuario sustraída (eventos 7 y 8).
- uso del usuario de emergencia no autorizado (evento 10).

Detalle de los eventos:

Para todos los sistemas de gestión de base de datos relacional y los usuarios con privilegios de administración

1) consultas a tablas de usuarios que no son propias del sistema.

2) incorporación, eliminación y/o modificación de datos en tablas de usuarios que no son propias del sistema.

3) asignación de altos privilegios a usuarios del sistema.

4) desbloqueo de cuentas de usuarios que fueron inhabilitados por indicación de seguridad informática. Por ejemplo, las cuentas de usuarios se inhabilitan cuando el mismo no asiste por un período superior a 90 días a la organización.

Para SAP ASE 16.0 SP01 y Teradata 13.10 y los usuarios con privilegios de administración

5) eliminación y modificación de registros de eventos de auditoria.

Para todos los sistemas de gestión de base de datos relacional y los usuarios desarrolladores

6) acceso de usuarios desarrolladores al entorno de producción.

Para todos los sistemas de gestión de base de datos relacional y la totalidad de usuarios

7) inicios de sesión fallidos.

8) posibles casos de claves compartidas.

9) uso de utilitarios para acceder a los datos (por ejemplo: empleo de los utilitarios bcp, cmd y bulk copy).

Para SAP ASE 16.0 SP01 y SQL Server 12 y los usuarios de emergencias

10) inicio de sesión del usuario SA.

4.1.7 Descripción general de los requerimientos

Se espera que se lleve a cabo:

- Establecer los diez eventos críticos desde el enfoque de la seguridad informática en los sistemas de gestión de base de datos relacional: Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10 contemplando los riesgos identificados en la organización.
- Identificar en la herramienta específica la modalidad en que se realizará el análisis de los diez eventos críticos definidos.
- Elaborar los procedimientos pertinentes para el análisis de los diez eventos críticos definidos.

4.1.8 Lista de los requerimientos

A continuación, se describen los requerimientos definidos durante las reuniones de extracción de requerimientos y elaborados en el análisis preliminar.

Nro	Requerimiento
1.	Analizar con la herramienta específica las consultas realizadas por los usuarios con privilegios de administración a tablas de usuarios que no son propias de los sistemas de gestión de base de datos relacional. Definir el procedimiento pertinente para el evento en cuestión.

2.	Analizar con la herramienta específica la incorporación, eliminación y/o modificación de datos en tablas de usuarios que no son propias de los sistemas de gestión de base de datos relacional por los usuarios con privilegios de administración. Definir el procedimiento pertinente para el evento en cuestión.
3.	Analizar con la herramienta específica la asignación de altos privilegios a usuarios de los sistemas de gestión de base de datos relacional. Definir el procedimiento pertinente para el evento en cuestión.
4.	Analizar con la herramienta específica el debloqueo de cuentas de usuarios de los sistemas de gestión de base de datos relacional que fueron inhabilitados por indicación de seguridad informática. Definir el procedimiento pertinente para el evento en cuestión.
5.	Analizar con la herramienta específica la eliminación y/o modificación de registros de eventos de auditoria de *SAP* ASE 16.0 SP01 y Teradata 13.10. Definir el procedimiento pertinente para el evento en cuestión.
6.	Analizar con la herramienta específica los accesos de desarrolladores al entorno de producción. Definir el procedimiento pertinente para el evento en cuestión.
7.	Analizar con la herramienta los inicios de sesión fallidos para los usuarios de todos los sistemas de gestión de base de datos relacional. Definir el procedimiento pertinente para el evento en cuestión.
8.	Analizar con la herramienta específica posibles casos de claves compartidas (actividad del mismo usuario desde distintas direcciones ip) para todos los sistemas de gestión de base de datos relacional. Definir el procedimiento pertinente para el evento en cuestión.
9.	Analizar con la herramienta específica el uso de los utilitarios bcp, cmd y bulk copy para acceder a los datos para todos los sistemas de gestión de base de datos relacional. Definir el procedimiento pertinente para el evento en cuestión.
10.	Analizar con la herramienta específica el inicio de sesión del usuario

	SA en SAP ASE 16.0 SP01 y SQL Server 12. Definir el procedimiento pertinente para el evento en cuestión.

4.2 Plan de trabajo

4.2.1 Antecedentes del proyecto

Alcance y restricciones

El presente plan de trabajo tiene como alcance analizar los diez eventos críticos desde el enfoque de la seguridad informática en Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10 utilizando una herramienta específica para este fin y definir los procedimientos pertinentes para los eventos en cuestión. No se incluyen las acciones o tratamientos de los posibles incidentes de seguridad detectados durante el análisis.

Las restricciones identificadas son:

- Por las características propias de la herramienta se requiere que para cada evento crítico se defina una política por cada sistema de gestión de base de datos relacional. Es decir que cada evento crítico podría tener asociadas cuatro políticas, una para SAP ASE, otra para Teradata, otra para Oracle y otra para SQL Server. La política establece el criterio con que se capturan los datos.
- Para solicitar la creación de las políticas asociadas a los eventos críticos se requiere la colaboración del administrador de la herramienta. Debido a que el mismo tiene a cargo la gestión de otros equipamientos de seguridad, pueden observarse demoras en las configuraciones requeridas.
- Para garantizar la disponibilidad de los eventos capturados por la herramienta se requiere del monitoreo del correcto funcionamiento de la misma.

Objetivo general

- Analizar con la herramienta específica los diez eventos críticos definidos para Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10.
- Definir los procedimientos de análisis de los diez eventos críticos definidos para Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10.

Objetivos específicos

Para Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10 y los usuarios con privilegios de administración, analizar con la herramienta específica, los eventos correspondientes a:

- consultas a tablas de usuarios que no son propias del sistema.
- incorporación, eliminación y/o modificación de datos en tablas de usuarios que no son propias del sistema.
- asignación de altos privilegios a usuarios del sistema.
- desbloqueo de cuentas de usuarios que fueron inhabilitados por indicación de seguridad informática.

Para SAP ASE 16.0 SP01, Teradata 13.10 y los usuarios con privilegios de administración

- eliminación y modificación de registros de eventos de auditoria

Para todos los sistemas de gestión de base de datos relacional y los usuarios desarrolladores

- acceso al entorno de producción

Para todos los sistemas de gestión de base de datos relacional y la totalidad de usuarios

- inicios de sesión fallidos
- posibles casos de claves compartidas
- uso de los utilitarios bcp, cmd y bulk copy para acceder a los datos.

Para SAP ASE 16.0 SP01, SQL Server 12 y los usuarios de emergencias

- inicio de sesión del usuario SA

Para todos los análisis de los eventos precedentes.

- elaborar los procedimientos pertinentes.

4.2.2 Planeamiento global del proyecto

Productos entregables

- Procedimiento de análisis de eventos de consultas a tablas de usuarios que no son propias de Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10 realizados por los administradores de base de datos.

- Procedimiento de análisis de eventos de incorporación, eliminación y/o modificación de datos en tablas de usuarios que no son propias de Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10 realizados por los administradores de base de datos.
- Procedimiento de análisis de eventos de asignación de altos privilegios a usuarios de Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10 realizados por los administradores de base de datos.
- Procedimiento de análisis de eventos de desbloqueo de cuentas de usuarios que fueron inhabilitados por indicación de seguridad informática en Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10 realizados por los administradores de base de datos.
- Procedimiento de análisis de eventos de eliminación y modificación de registros de eventos de auditoria en SAP ASE 16.0 SP01 y/o DBQL de Teradata 13.10 realizados por los administradores de base de datos.
- Procedimiento de análisis de eventos de inicios de sesión de usuarios del área de desarrollo en el entorno de producción de Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10.
- Procedimiento de análisis de eventos de inicios de sesión fallidos para todos los usuarios de Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10.
- Procedimiento de análisis de eventos de posibles casos de claves compartidas para todos los usuarios de Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10.
- Procedimiento de análisis de eventos del uso de los utilitarios bcp, cmd y bulk copy para acceder a los datos por parte de todos los usuarios de Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10.
- Procedimiento de análisis de eventos del inicio de sesión del usuario SA de SAP ASE 16.0 SP01 y/o SQL Server 12.
- Informe de situación actual al cierre del proyecto.

Fases a cumplimentar

Las siguientes fases se aplican para cada uno de los eventos críticos definidos para Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10

1. Identificar las variables técnicas que intervienen en cada evento crítico definido, a saber:

- Sistema de gestión de base de datos relacional
- Usuarios que ejecutan el evento
- Eventos propios del sistema de gestión de base de datos relacional que corresponden a los eventos a analizar.

Por ejemplo: para el evento crítico correspondiente al inicio de sesión del usuario SA, las variables técnicas son:

- Sistema de gestión de base de datos relacional: SAP ASE 16.0 SP01 y SQL Server 2012.
- Usuarios: cuenta SA
- Eventos propios del sistema de gestión de base de datos relacional que corresponden a las acciones a detectar: evento de login tanto para SAP ASE 16.0 SP01 como en SQL Server 2012.

2. Definir en conjunto con el administrador de la herramienta la implementación óptima.
3. Implementar el análisis del evento crítico en la herramienta específica.
4. Realizar un seguimiento de la implementación en la herramienta específica. Solicitar ajustes en caso de corresponder y brindar la conformidad al administrador de la herramienta.
5. Elaborar el procedimiento de análisis del evento crítico.
6. Cierre del proyecto.

4.2.3 Planeamiento detallado del proyecto

Definición de actividades y tareas

Para identificar a las actividades se utiliza la letra A y el número de la actividad.

Actividad	Tarea
A1 Identificar las variables técnicas que intervienen en cada evento crítico definido.	• Para el evento de consulta a tablas de usuarios que no son propias del sistema de gestión de

	base de datos relacional, se debe identificar para Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10 los usuarios con privilegios de administración, las tablas propias del sistema y el evento correspondiente a la consulta (select). • Para el evento de incorporación, eliminación y/o modificación de datos en tablas de usuarios que no son propias del sistema de gestión de base de datos relacional, se debe identificar para Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10 los usuarios con privilegios de administración, las tablas propias del sistema y los eventos correspondientes (insert, delete y update). • Para el evento de asignación de altos privilegios a usuarios del sistema de gestión de base de datos relacional, se debe identificar para Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata las características de los altos privilegios en cada sistema y el evento correspondiente (grant). • Para el evento de desbloqueo de cuentas de usuarios que fueron inhabilitados por indicación de seguridad informática en los

	sistemas de gestión de base de datos relacional, se debe identificar para Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10 el evento correspondiente al desbloqueo de usuario (alter user, sp_locking, alter login y modify user). • Para el evento de eliminación y modificación de registros de eventos de auditoria, se debe identificar para SAP ASE 16.0 SP01 y Teradata 13.10 las tablas utilizadas para el resguardo de las pistas de auditoria y los eventos correspondientes (delete, truncate table). • Para el evento de inicios de sesión de usuarios del área de desarrollo en el entorno de producción en los sistemas de gestión de base de datos relacional, se debe identificar para Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10 los usuarios desarrolladores y el evento correspondiente (inicio de sesión, action=100, audit login, event=45, help session). • Para el evento correspondiente a los inicios de sesión fallidos de usuarios en los sistemas de gestión de base de datos relacional, se debe identificar para Oracle 11 g r2, SAP

	ASE 16.0 SP01, SQL Server 12 y Teradata 13.10 evento correspondiente y el umbral de control para clasificar el evento como incidente de seguridad. • Para el evento correspondiente a posibles casos de claves compartidas en los sistemas de gestión de base de datos relacional, se debe identificar para Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10 el uso de una cuenta de usuario desde diferentes direcciones ip. • Para el evento correspondiente a la detección de los utilitarios bcp, cmd, bulk copy para acceder a los datos de los sistemas de gestión de base de datos relacional, se debe identificar para Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10 el evento correspondiente. • Para el evento correspondiente a detectar el inicio de sesión del usuario SA, se debe identificar para SAP ASE 16.0 SP01 y SQL Server 12 el evento correspondiente.
A2 Definir en conjunto con el administrador de la herramienta la implementación óptima.	Para cada evento crítico definido se debe: • Presentar un requerimiento al administrador de la herramienta. • Efectuar reuniones con el

	administrador de la herramienta para analizar las alternativas. • Acordar la modalidad de la implementación.
A3 Implementar el análisis del evento crítico en la herramienta específica.	Para cada evento crítico definido se debe: • Efectuar las configuraciones acordadas en la herramienta.
A4 Homologar la implementación del evento crítico en la herramienta específica.	Para cada evento crítico definido se debe: • Analizar el resultado de la configuración efectuada por el administrador de la herramienta. • Solicitar ajustes en caso de corresponder. • Brindar la conformidad de la implementación.
A5 Elaborar el procedimiento de análisis del evento crítico.	Para cada evento crítico definido se debe: • Elaborar el procedimiento de análisis del evento crítico utilizando la herramienta específica.
A6 Realizar el cierre de proyecto	Elaborar un informe de situación actual al finalizar el proyecto.

Secuencia temporal de actividades

Para cada uno de los eventos críticos definidos se ejecutan en forma secuencial las actividades: A1, A2, A3, A4 y A5.

En la actividad A1 debe aplicarse solo los puntos que correspondan al evento en cuestión.

Al finalizar todas las implementaciones en producción se ejecutará el cierre del proyecto (A6).

Recursos asociados a actividades

Los recursos asociados a las actividades A1, A2, A3, A4 y A5 aplican a un evento crítico definido.

Se acota que el cálculo financiero solamente considera la cantidad de horas requeridas por actividad.

Las estimaciones de los recursos que se presentan en la siguiente tabla corresponden a un evento crítico, con excepción de la actividad A6.

Actividad	**Recursos**			
	Humanos	**Material**	**Técnicos**	**Financiero**
A1	2 Analistas Senior de Seguridad Informática 1 Líder de proyecto 1Administrador de base de datos	Oficina de reuniones Escritorios de trabajo Impresora Papel	Acceso a internet Computadora Manuales técnicos Servidores del entorno de homologación que cuenten con los sistemas de gestión de base de datos relacional	16 hs por cada Analistas Senior de Seguridad Informática **Total**: 32 hs 4 h de Líder de proyecto **Total**: 4 hs 16 hs de administrador de base de datos **Total:** 16 hs
A2	2 Analistas Senior de Seguridad Informática 1 Líder de proyecto 1aministrador de la herramienta de análisis	Oficina de reuniones Escritorios de trabajo Impresora Papel	Acceso a internet Computadora Manuales técnicos Acceso a la herramienta de análisis	16 hs por cada Analistas Senior de Seguridad Informática **Total**: 32 hs 5 hs de Líder de proyecto **Total**: 5 hs 16 hs de administrador de la herramienta de análisis **Total:** 16 hs
A3	1 Líder de proyecto 1aministrador de la herramienta de	Oficina de reuniones Escritorios de trabajo Impresora	Acceso a internet Computadora Manuales técnicos	16 hs de administrador de la herramienta de análisis **Total**: 16 hs

	análisis	Papel	Acceso a la herramienta de análisis	3 hs de Líder de proyecto **Total**: 3 hs
A4	2 Analistas Senior de Seguridad Informática 1 Líder de proyecto 1aministrador de la herramienta de análisis	Oficina de reuniones Escritorios de trabajo Impresora Papel	Acceso a internet Computadora Manuales técnicos Acceso a la herramienta de análisis	24 hs por cada Analistas Senior de Seguridad Informática **Total**: 48 hs 6 hs de Líder de proyecto **Total**: 6 hs 24 hs por cada administrador de base de datos **Total:** 24 hs
A5	1 Analista Senior de Seguridad Informática 1 Líder de proyecto	Oficina de reuniones Escritorios de trabajo Impresora Papel	Acceso a internet Computadora Manuales técnicos Acceso a la herramienta de análisis	8 hs de Analista Senior de Seguridad Informática **Total**: 8 hs 1 hs de Líder de proyecto **Total**: 1 hs
A6	1 Líder de proyecto	Escritorios de trabajo Impresora Papel	Acceso a internet Computadora	24 hs de Líder de proyecto **Total**: 24 hs

Costos del proyecto

Costos por fase

Los costos son expresados en horas.

Fase	**Costo en horas por evento crítico**	**Costo total en horas del proyecto (10 eventos críticos)**
A1	52	520
A2	53	530
A3	19	190
A4	78	780
A5	9	90
A6	24	24

Plan de Adquisiciones y contrataciones

El proyecto se realiza con personal y recursos materiales de la organización no se requieren adquisiciones ni contrataciones.

Costo total y duración total

El costo total es de 2134 horas y la duración total es de aproximadamene 21 semanas.

Criterios de calidad y análisis de riesgos
Identificación de riesgos

Los principales riesgos identificados son:

1. Desafectación de recursos humanos. Reasignación de nuevas tareas a los recursos humanos participantes del proyecto.
2. Los tiempos dedicados al proyecto no son los suficientes
3. Dificultad técnica en adquirir el conocimiento necesario para concretar los productos esperados.
4. Falta de herramientas técnicas, administrativas y operativas a utilizar.

4.3 Informe de situación final

Para confeccionar el siguiente informe se consultó el sitio de internet mencionado en la referencia [18].

Se efectuaron satisfactoriamente, en tiempo y forma los siguientes trabajos:

- Análisis de los diez eventos críticos definidos para Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10 con la herramienta específica. Se destaca que para los siguientes eventos fue factible utilizar las consultas por defecto que provee la herramienta:

Evento	**Funcionalidad de la herramienta de análisis**
Asignación de altos privilegios a usuarios de los sistemas de gestión de base de datos relacional	Privileged Operations /DCL Command

Desbloqueo de cuentas de usuarios	Privileged Operations /DCL Command
Eliminación y/o modificación de registros de eventos de auditoria de SAP ASE 16.0 SP01 y Teradata 13.10	Privileged Operations / Table drops /truncates
Detección de gran cantidad de inicios de sesión fallidos	Additional Views/ Failed Login
Detección de posibles casos de claves compartidas	Source Analysis/ Login Análisis
Detección del uso de los utilitarios bcp, cmd y bulk copy para acceder a los datos	Source Analysis/ Source Application

Para el resto de los eventos, se configuraron políticas específicas con los filtros identificados. Dichas políticas pueden ser consultadas desde la interface gráfica de la herramienta de análisis de eventos.

- Elaboración de los procedimientos para el análisis de los diez eventos críticos utilizando la herramienta específica para el análisis.

Dificultades encontradas

Se observa como dificultad el mantenimiento de las políticas que capturan los eventos objeto del análisis. Si se produce cualquier cambio en las variables utilizadas en el filtro de la política definida, la misma perdería vigencia y el resultado del análisis del evento sería insatisfactorio. Por ejemplo: para el evento crítico correspondiente al acceso de desarrolladores al entorno de producción se definió una política que contiene en el filtro el listado del personal del sector de desarrollo. Si se presentan variaciones entre los integrantes del área de desarrollo, tal como una nueva incorporación al sector y este cambio no es actualizado en el filtro de la política, la misma no será efectiva y el análisis del evento será insastifactorio.

Adicionalmente, se identificó que eventualmente se podría generar una gran cantidad de eventos en los sistemas de gestión de base de datos relacional lo que incrementaría el volumen de eventos enviados a la

herramienta específica. Dicha situación podría generar posibles pérdidas de eventos si se supera el ancho de banda de la red y/o demoras en el procesamiento de la herramienta. Ante lo expuesto, se requiere que se implementen medidas de monitoreo permanente para garantizar la disponibilidad de los eventos en la herramienta de análisis.

En particular para Teradata 13.10 se presentaron dificultades en la captura de eventos dado que los eventos no contaban con la descripción del usuario que ejecutó el evento. Esta situación fue resuelta en conjunto entre el fabricante del sistema de gestión de base de datos relacional y el fabricante de la herramienta.

Por otro lado, para SQL Server 2012 fue necesario configurar en la herramienta de análisis el certificado digital que utilizan las aplicaciones implementadas con protocolo SSL.

Relaciones con terceros

No se presentaron dificultades entre los sectores intervenientes.

En particular, en algunas ocasiones se requirió consultar al fabricante de la herramienta específica de análisis de eventos para configurar las políticas relacionadas con los eventos críticos definidos.

Acciones futuras

Con el fin de incrementar el uso de las funcionalidades de la herramienta específica de análisis de eventos se incorporará el análisis de nuevos eventos críticos relacionados con los resultados del proceso de clasificación de la información.

Asimismo, se requiere definir un circuíto para el mantenimiento de las políticas de captura de eventos configuradas en la herramienta específica.

Resumen del estado:

	SI	**NO**
Modificaciones al alcance		x
Retrasos		x
Incremento del riesgo		x

Sobrecoste	x
Insatisfacción del Cliente	x
Ampliaciones al contrato	x
Carencia de recursos	x
Conflictos interpersonales	x
Falta de formación y/o experiencia	x

Capítulo V

En el presente capítulo se llevó a cabo un relevamiento sobre los cambios tecnológicos en los sistemas de gestión de base de datos relacional vigentes en el mercado debido a que la elaboración de los capítulos I, II, III y IV se finalizó en junio de 2016. Se acota que solo se analizaron los aspectos relacionados con la configuración y análisis de registros de eventos de auditoria.

A continuación, se presentan los resultados obtenidos:

La última versión de Teradata en el mercado corresponde a la 16.0. Esta versión ofrece las siguientes mejoras en comparación con la versión 13.10 mencionada en el presente trabajo:

- disponibilidad del script IPPDCR y el Viewpoint portlet Performance Data Collection para ser utilizados en el mantenimiento de las tablas temporales y las tablas históricas DBQL.
- posibilidad de utilizar otras opciones para registrar eventos, a través de la opción WITH de la sentencia BEGIN/REPLACE QUERY LOGGING. Por ejemplo, se pueden registrar los eventos después de un bloqueo de determinadas centésimas de segundos.
- incorporación de nuevos campos en DBQLogTbl y QryLogV que brindan mayor de detalle del registro de eventos de auditoria.
- cambios en tablas y vistas del diccionario de datos de DBQL.

En resumen, Teradata incrementó el nivel de detalle en el registro de eventos de auditoría y mejoró la gestión de las tablas temporales y tablas históricas DBQL. [19]

La última versión de SAP Adaptive Server Enterprise es 6.0 SP03 PL02. Esta versión no presenta cambios en la configuración y análisis de registros de eventos de auditoría en relación a la versión analizada en el presente trabajo. [20]

La última versión de SQL Server es la 16. En particular, todas las ediciones de SQL Server soportan el registro de eventos de auditoría a nivel de servidor. Desde SQL Server 2016 SP 1 todas las ediciones soportan auditoría a nivel de base de datos, antes de esto, la auditoría a nivel de base

de datos estaba limitada a las ediciones Enterprise, Developer y Evaluation. [21]

En conclusión, SQL Server incrementó su funcionalidad de registro de eventos a nivel de bases de datos a todos sus tipos de ediciones. Esta situación permite que se registren eventos de auditoria a nivel de bases de datos en las ediciones más económicas de SQL Server.

La última versión de Oracle es la 12 c release 2. Esta versión no presenta cambios en la configuración y análisis de registros de eventos de auditoría con respecto lo enunciado en el presente trabajo. [22]

En cuanto, a la herramienta específica para el análisis de eventos de auditoria de los sistemas de gestión de base de datos relacional mencionada en el capítulo IV, se verificó que dicho producto se encuentra vigente en el mercado y soporta las bases de datos correspondientes a Teradata, SAP Adaptive Server Enterprise, SQL Server y Oracle, entre otras. [32]

Finalmente, se concluye que es factible implementar las configuraciones y los análisis de los registros de eventos descriptos en el capítulo III en las actuales versiones de Teradata, SAP Adaptive Server Enterprise, SQL Server y Oracle vigentes en el mercado e implementar la herramienta específica de análisis indicada en el capítulo IV del presente trabajo.

Conclusión

Se destaca que el presente trabajo final fue elaborado bajo el enfoque de orientación profesional y se focalizó en definir los lineamientos de configuración y análisis de los registros de eventos de auditoria en los sistemas de gestión de bases de datos relacional para una organización específica.

Como resultado del trabajo efectuado se concluye que la configuración y el análisis de los registros de eventos de auditoria de los sistemas de gestión de base de datos relacional permiten a la organización conocer las acciones realizadas sobre sus datos, identificando quien accedió, cuándo, qué actividad realizó y cómo la llevo a cabo. Disponer de esta información permite a la organización detectar las situaciones que comprometan a la seguridad de la información y definir posteriormente los controles preventivos y correctivos pertinentes.

Del análisis del marco teórico conceptual del capítulo I se observó que la configuración del registro de eventos de auditoria en los productos comerciales Oracle 12 C, SQL Server 12, SAP ASE 16.0 SP01 y Teradata 13.10 se realiza técnicamente en forma diferente en cada uno de ellos con requisitos particulares y requiere de especialistas para su implementación.

En cuanto al análisis de los eventos registrados, se observa que los eventos de auditoria son guardados en distintos formatos y para su consulta se necesita que el operador tenga conocimientos detallados de las estructuras y el contenido de los repositorios de eventos. Asimismo, se requiere implementar un mecanismo de análisis diferente con sus respectivas tareas operativas para cada sistema de gestión de base de datos relacional. Al respecto, se concluye que no es factible aplicar un mismo procedimiento para realizar la configuración y el análisis de registro de eventos en Oracle12 C, SQL Server 12, SAP ASE 16.0 SP01 y Teradata 13.10.

En relación a la comparación efectuada en el capítulo II, se observó:

- SQL Server y Oracle son mas flexibles porque ofrecen mas de una alternativa para la configuración del registro de eventos de auditoria en

comparación con SAP ASE y Teradata. Estos últimos solo disponen de una única variante para dicha funcionalidad.

- Teradata registra los eventos a nivel de usuario. Los otros productos presentan mas opciones, tales como registrar eventos a nivel de servidor, base de datos y sentencias, entre otros. Esta particularidad dificulta la aplicación de un criterio homogéneo para el registro de eventos en todos los productos involucrados.
- SQL Server es el único que requiere el reinicio del servicio para habilitar el registro de los eventos de auditoria en sus opciones C2, Common Criteria Compliance, SQL Trace y SQL Audit. Esta característica implica que la habilitación del registro de eventos condicione la disponibilidad del servicio. En los otros casos el registro de eventos de auditoria se activa sin comprometer la disponibilidad del servicio.
- Oracle y SQL Server pueden guardar los eventos de auditoria en archivos externos, tablas predefinidas, tablas definidas por usuarios o en el registro de eventos del sistema operativo. En particular, SQL Server puede generar archivos de extensión trc que tienen un formato propietario de Microsoft y requiere de herramientas específicas para su consulta y Oracle en su opción de auditoria unificada guarda los datos en tablas de solo lectura. Por otro lado, SAP ASE y Teradata únicamente guardan los eventos en tablas de estructuras predefinidas. Al respecto, se debe tener en cuenta que un usuario con privilegios de administración podría eliminar o modificar los eventos de auditoria en SAP ASE, Teradata, SQL Server en la modalidad trigger o SQL Trace si se optó por guardar los eventos en una tabla y Oracle en sus opciones básica si se optó por guardar los eventos en una tabla o en la funcionalidad FGA. Para estos casos se deben implementar controles específicos para detectar dicha situación que compromete la integridad y confidencialidad de los eventos registrados.
- SAP ASE, Teradata y SQL Server con sus opciones de SQL Trace y SQL Audit permiten automatizar la gestión de almacenamiento y depuración de los registros de eventos a través del empleo de procedimientos almacenados, tablas predefinidas o configuración de parámetros. En particular, Oracle en la opción de auditoria unificada solo cuenta con un procedimiento almacenado para liberar las colas donde se encuentran los

eventos de auditoria. En SQL Server en sus modalidades de C2, Common Criteria Compliance y trigger y Oracle en sus modalidades básica, auditoria de Sysdba y de usuarios Sysoper y funcionalidad FGA requieren diseñar e implementar tareas operativas para el almacenamiento y depuración de los registros de eventos. Dichas tareas incrementan los costos y precisan de un monitoreo para garantizar su correcto funcionamiento.

- SAP ASE y SQL Server en sus opciones SQL Trace, triggers y SQL Audit cuentan con la posibilidad de agregar registros a los eventos de auditoria. Dicha característica ocasiona que se deban definir los procedimientos pertinentes para autorizar la incorporación de los eventos de auditoria.
- SAP ASE, Teradata, Oracle y SQL Server cuentan con tablas, vistas o comandos que permiten consultar las opciones de registro de eventos activas lo que permite verificar que se encuentren habilitadas las opciones correspondientes.
- SAP ASE requiere que se asigne el rol SSO al operador que consulta los eventos de auditoria. Esta característica ocasiona que el usuario que consulta los eventos registrados tenga mayores privilegios de los que necesita. Para Oracle, Teradata y SQL Server es factible limitar los permisos de los usuarios que consultan los eventos de auditoria registrados.
- Los registros de eventos en SAP ASE, Teradata, Oracle y SQL Server brindan información con diferentes niveles de detalles sobre quien ejecutó el evento, cuando y que hizo. En particular Teradata, SQL Server y Oracle en su opción de auditoria unificada brindan información sobre como se efectuó el evento. Por otro lado, SAP ASE no dispone de un campo específico que informe como se realizó un evento, eventualmente este tipo de información se puede encontrar en el campo que contiene información adicional del evento. Con respecto a Oracle se observa que no dispone de información sobre como se llevó a cabo el evento en sus modalidades básica, auditoria de Sysdba y de usuarios Sysoper y funcionalidad FGA. En conclusión, SAP ASE y Oracle en sus modalidades básica, auditoria de Sysdba y de usuarios Sysoper y funcionalidad FGA observan limitaciones en la información suministrada sobre cómo se ejecutó el evento.
- Teradata es el producto que ofrece mayor información sobre cuando se ejecutó el evento. Brinda en detalle distintas fechas y horarios relacionados

con el evento registrado. Adicionalmente, incluye información sobre el rendimiento técnico.

- Los registros de eventos de SAP ASE, Teradata, SQL Server y Oracle cuentan con información detallada sobre que se hizo en el evento registrado, indicando al menos que evento se ejecutó, el objeto y la base de datos a la que se accedió y el resultado de la operación.

El resultado de la comparación de Oracle 12 c, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10 aporta información valiosa de los siguientes aspectos:

- requerimientos del script de instalación para habilitar la funcionalidad del registro de eventos de auditoria.
- privilegios necesarios para la instalación.
- comandos utilizados para la configuración del registro de eventos de auditoria.
- privilegios necesarios para la configuración.
- niveles de auditoria a habilitar.
- factibilidad de realizar la configuración en línea sin interrupción del servicio.
- repositorio de los eventos registrados.
- gestión del almacenamiento y depuración de los registros de eventos.
- posibilidad de agregar nuevos eventos a los registrados.
- posibilidad de consultar las opciones de auditorias habilitadas.
- mecanismo disponible para el análisis de los eventos registrados.
- privilegios necesarios para la consulta de los eventos registrados.
- identificación en el registro de evento de auditoria de quién, cuándo y cómo realizó el evento y que acción se efectuó.

Se destaca que dicha información permite conocer las fortalezas y limitaciones de los productos comparados. Por otro lado, en futuras investigaciones un tema interesante a tratar sería efectuar la comparación de la configuración y el análisis de los registros de eventos de auditoría en las nuevas versiones de los productos comerciales Oracle, SAP ASE, SQL Server y Teradata y analizar su evolución desde los resultados obtenidos en el presente trabajo.

En cuanto a la implementación de la configuración y el análisis de los registros de eventos de auditoría de Oracle 11 g r2, SAP ASE 16.0 SP01,

SQL Server 12 y Teradata 13.10 en una organización específica, enunciado en el capítulo III, se observó que para cada sistema de gestión de base de datos relacional fue necesario realizar un análisis para determinar la modalidad de configuración a implementar. Dicho análisis contempló la dificultad técnica de su implementación, el impacto que tendría en el servidor la habilitación del registro de eventos, la protección de la integridad de los eventos registrados y la dificultad del análisis de los eventos registrados. Adicionalmente, se requirió seleccionar los eventos a registrar según los riesgos identificados en la organización debido a que no se recomienda habilitar el registro de la totalidad de los eventos. Los eventos seleccionados corresponden a la totalidad de las acciones de los administradores de las bases de datos y los inicios de sesión exitosos y fallidos de la totalidad de los usuarios para SAP ASE 16.0 SP01 y SQL Server 12. En cuanto a Teradata 13.10 se registran las acciones de los administradores de las bases de datos y en Oracle 11 g r2 se registran los inicios de sesión exitosos y fallidos de la totalidad de los usuarios y las acciones de los administradores de las bases de datos exceptuando los eventos de select, insert, delete y update. En resumen, se efectuó satisfactoriamente:

- La configuración del registro de eventos de auditoría en Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10 logrando que el impacto de la configuración no comprometa en mas de un 10% el rendimiento de los servidores.
- La implementación de los procesos de almacenamiento y depuración de los registros de eventos en todos los sistemas de gestión de base de datos relacional con el fin de evitar pérdidas de eventos y disponer de los mismos para consultas futuras.
- La definición de los controles pertinentes para detectar eliminaciones de pistas de auditoria en SAP ASE 16.0 SP01 y Teradata 13.10.
- La definición del tratamiento de excepciones para agregar registros de eventos de auditoria en SAP ASE 16.0 SP01 y SQL Server 2012.
- La definición de los procedimientos para el análisis de los eventos registrados en los sistemas de gestión de base de datos relacional. En cuanto al análisis, en todos los productos comerciales contemplados y para las opciones de registro establecidas en el capítulo III, se concluye que es

factible interpretar satisfactoriamente el contenido de los eventos. La calificación de satisfactorio, es sobre una escala de: insatisfactorio, satisfactorio y muy satisfactorio. Sin embargo, se considera que la tarea de análisis tiene un alto costo operativo debido a la heterogeneidad de los datos registrados y la detección del evento no deseado podría no ser lo suficientemente oportuna para la implementación de las medidas correctivas y preventivas apropiadas para mitigar los riesgos de la organización.

Se destaca que al finalizar el proyecto la organización incrementó sus niveles de seguridad al disponer de los registros de eventos de auditoria y contar con la información necesaria para definir los cursos de acción preventivos y de detección que considere necesarios para mitigar los riesgos.

Finalmente, en el capítulo IV se describieron las tareas realizadas para efectuar el análisis de los diez eventos críticos definidos para Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10 utilizando una herramienta específica. En particular, los diez eventos definidos por la organización son:

Para Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10 y los usuarios con privilegios de administración:

- consultas a tablas de usuarios que no son propias del sistema.
- incorporación, eliminación y/o modificación de datos en tablas de usuarios que no son propias del sistema.
- asignación de altos privilegios a usuarios del sistema.
- desbloqueo de cuentas de usuarios que fueron inhabilitados por indicación de seguridad informática.

Para SAP ASE 16.0 SP01, Teradata 13.10 y los usuarios con privilegios de administración

- eliminación y modificación de registros de eventos de auditoria.

Para todos los sistemas de gestión de base de datos relacional y los usuarios desarrolladores

- acceso al entorno de producción.

Para todos los sistemas de gestión de base de datos relacional y la totalidad de usuarios

- inicios de sesión fallidos.
- posibles casos de claves compartidas.
- uso de los utilitarios bcp, cmd y bulk copy para acceder a los datos.

Para SAP ASE 16.0 SP01, SQL Server 12 y los usuarios de emergencias

- inicio de sesión del usuario SA

En resumen, se efectuó satisfactoriamente:

- El análisis de los diez eventos críticos definidos para Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10 utilizando la herramienta específica.
- La definición de los procedimientos de análisis de los diez eventos críticos definidos para Oracle 11 g r2, SAP ASE 16.0 SP01, SQL Server 12 y Teradata 13.10.

En particular, para seis eventos fue factible utilizar las consultas por defecto que provee la herramienta. Para los otros eventos se necesitó configurar las políticas específicas con los filtros correspondientes.

Se considera que el uso de una herramienta específica para el análisis de eventos facilita dicha tarea y permite agilizar la detección de eventos no deseados. Por otro lado, se considera que la adquisición de una herramienta de análisis de eventos tiene un costo monetario considerable y altamente superior al uso de las auditorias por defecto que traen los sistemas de gestión de base de datos relacional. En consecuencia, la organización debe analizar si la inversión justifica los beneficios a obtener. Se considera que una herramienta de análisis de eventos es recomendable para contextos que deben cumplir con marcos regulatorios y realizan tareas avanzadas de análisis de eventos y gestión de incidentes.

Se resalta que al concluir el proyecto la organización logró disminuir los tiempos que requería para efectuar las tareas de análisis de los registros de eventos de auditoria, los tiempos de detección de las situaciones no deseadas que comprometen la seguridad de la información y los tiempos de respuestas ante dichas situaciones.

Adicionalmente, en el capítulo V, en abril de 2018 se realizó un relevamiento sobre los cambios tecnológicos en los sistemas de gestión de base de datos relacional descriptos en el capítulo III y en la herramienta de

análisis de eventos indicada en el capítulo IV. De dicho análisis, se concluyó que es factible implementar las configuraciones y los análisis de los registros de eventos descriptos en el capítulo III en las actuales versiones de Teradata, SAP Adaptive Server Enterprise, SQL Server y Oracle e implementar la herramienta específica de análisis de eventos de auditoria indicada en el capítulo IV del presente trabajo.

Anexo I: Opciones de las teglas de registro de eventos de Teradata

Detalle de la opción WITH

Opción DBQL	Detalle	Tabla que registra la información
WITH ALL	Registra toda la información generada por las reglas ((EXPLAIN, OBJECTS, SQL y STEPINFO) excepto XMLPLAN. Las opciones de WITH ALL genera: • Una fila por cada consulta en DBQLogTbl que incluye los primeros 200 caracteres de la declaración SQL, a menos que se defina LÍMITE SQLTEXT = 0. • Una fila por cada objeto de destino de la consulta en la tabla DBQLObjTbl. • Una fila por cada paso de la consulta en la tabla DBQLStepTbl. • Una o más filas por sentencia SQL en la tabla DBQLSQLTbl. • Una o más filas por la consulta en la tabla DBQLExplainTbl.	DBC.DBQLogTbl BC.DBQLExplainTbl DBC.DBQLObjTbl DBC.DBQLStepTbl DBC.DBQLSQLTbl
WITH EXPLAIN	La tabla DBQLExplainTbl se completa con un texto sin formato el cual se denomina EXPLAIN. Si el texto EXPLAIN es mayor que 64KB, se generan varias filas y el campo ExpRowNo indica el número de la fila correspondiente. Esta opción inserta una fila por defecto en DBQLogTbl. Nota: No se puede especificar la opción WITH EXPLAIN con las opciones SUMMARY o THRESHOLD.	DBC.DBQLogTbl DBC.DBQLExplainTbl
WITH OBJEC	Esta opción inserta:	DBC.DBQLogTbl

TS	• Una fila por defecto en DBQLogTbl. • Una fila por cada objeto de destino de la consulta en la tabla DBQLObjTbl. Teradata recomienda usar esta opción en forma selectiva debido a que se pueden generar muchas filas en la tabla DBQLObjTbl. Esta opción se puede utilizar con las opciones SUMMARY o THRESHOLD. Nota: Cualquier tabla de la base de DBC y las columnas utilizadas por el sistema para procesar una consulta no son reflejado en las filas de objetos DBQL. Si una instrucción accede a una tabla DBC, la tabla DBC no aparecerá en DBQLObjTbl.	DBC.DBQL ObjTbl
WITH NONE	Esta opción ocasiona que no se registren eventos de un usuario especificado, cuenta o aplicación. Por ejemplo, si hay una regla de registro sobre todos los usuarios, se puede excluir el registro para un usuario específico, mediante la siguiente declaración: BEGIN QUERY LOGGING WITH NONE ON user1;	Ninguna.
WITH SQL	Esta opción agrega: • Una fila por defecto en DBQLogTbl. • La sentencia completa de SQL para cada solicitud de cada usuario que se está registrando. Se debe tener en cuenta que las sentencias largas pueden generar varias filas. Nota: Esta opción se puede utilizar con la opción THRESHOLD que limita la captura de la información. Si se establece LIMIT SQLTEXT igual a 0 cuando se especifica la opción WITH SQL, se puede	DBC.DBQLo gTbl BC.DBQLSQ LTbl

	evitar duplicados SQL en el DBQLogTbl.	
WITH STEPINFO	Completa la DBQLStepTbl con información a nivel de AMP para todas las consultas SQL realizadas por un usuario especificado. La opción WITH STEPINFO inserta una fila por defecto en DBQLogTbl. Nota: Esta opción se puede utilizar con THRESHOLD.	DBC.DBQLogTbl DBC.DBQLStepTbl
WITH XMLPLAN	Esta opción sólo registra la información de las sentencias DML, incluyendo INSERT, UPDATE, DELETE, SELECT, MERGE y EXEC en DBQLXMLTbl e inserta una fila por defecto en DBQLogTbl. Debido a que el plan de XML incluye la consulta y la explicación del texto, Teradata recomienda que cuando se utiliza la opción XMLPLAN, no se utilice también WITH EXPLAIN y WITH SQL. Se recomienda establecer la opción SQLTEXT igual a 0 para evitar redundancia de registro si una consulta y un texto explicado no son requeridos por una sentencia DDL. Nota: Esta opción no se puede utilizar con THRESHOLD ni RESUME.	DBC.DBQLogTbl DBC.DBQLXMLTbl DBC.DBQLExplainTbl

Las limitaciones que controlan la cantidad y cuando los eventos son registrados en DBQLogTbl y DBQLSummaryTbl son:

Parámetro	**Comportamiento del registro**
LIMIT SQLTEXT	Esta opción permite definir cuanto texto de SQL se captura para ser registrado en DBQLogTbl. Para que no se capture ningún texto se debe completar esta opción con valor cero. La sintaxis es LIMIT SQLTEXT=n, donde n es un valor mayor a cero que representa a la cantidad de

<table>
<tr><td></td><td>caracteres. El límite máximo es 10000 caracteres.
Para guardar sentencias mayores a esta longitud se debe habilitar la opción WITH SQL que permite registrar mas de una fila.
Si se utiliza la opción WITH SQL y se debe definir LIMIT SQLTEXT=0 para evitar la redundancia del registro.</td></tr>
<tr><td>LIMIT SUMMARY</td><td>Esta opción permite definir la cantidad de las consultas basados sobre el tiempo, AMP, CPU o diferentes entradas/salidas y guardar el resultado en DBQLSummaryTbl.
Esta opción:
No genera una fila por defecto en DBQLogTbl.
Vacía la información resumida a intervalos controlados por el sistema de 10 minutos.
No escribe filas si no se han recopilado para su registro en un intervalo de 10 minutos.
Esta opción es útil para el seguimiento de las consultas voluminosas.</td></tr>
<tr><td>LIMIT THRESHOLD</td><td>Las consultas que corren en “n” unidades o menos son contadas en DBQLSummaryTbl.
Las consultas que corren sobre “n” unidades se registran en DBQLogTbl. Las unidades pueden ser: CPUTIME, CPUTIMENORM, ELAPSEDSEC, ELAPSEDTIME, IOCOUNT
La definición de un umbral determinará si desea registrar una consulta o simplemente contarla, de la siguiente manera:<table><tr><th>Si una consulta</th><th>Luego DBQL</th></tr><tr><td>Se completa hasta o por debajo del umbral de tiempo transcurrido, segundos de CPU, o contador de I / O</td><td>Incrementa el número de consultas y añade el tiempo transcurrido de la consulta, tiempo de CPU y contador de E / S a la fila de resumen</td></tr></table></td></tr>
</table>

		para esta sesión en el período actual de recolección. Almacena el conteo final para la sesión con una fila en DBQLSummaryTbl. En la fila resumen, establece en el campo LowHist el tiempo del umbral (THRESHOLD) y al campo HighHist en cero.
	Se ejecuta más allá del valor definido en el umbral	Registra una fila por defecto para la consulta en DBQLSqlTbl, DBQLStepTbl, Y DBQLogTbl. Se puede examinar su tiempo de ejecución a través de la estampo o sello de tiempo, el número y el nivel de procesamiento.

Anexo II: Detalle de las tablas BDQL, vistas y macros de Teradata

Tabla DBQLogTbl

La principal tabla de registro de eventos es DBQLogTbl. Por defecto una fila guarda una consulta.

Se puede limitar el registro a través de las opciones:

LIMIT THRESHOLD: reduce la cantidad de filas registradas a una cantidad menor o igual al umbral definido. El resto de las filas se guardan en DBQLSummaryTbl.

LIMIT SUMMARY: elimina los registros de filas por defecto.

Además, al registro de eventos por defecto se puede especificar la opción WITH para registrar OBJECTS, SQL, STEPINFO y/o EXPLAIN. El LIMIT THRESHOLD puede aceptar combinaciones de SQL, STEPINFO y/o OBJECTS. Se debe tener en cuenta que si se especifican las opciones WITH esto resulta en información con mayor detalle.

La composición de los campos de cada fila de DBQLogTbl es la siguiente:

Campo	Descripción
ProcID	Número de identificación único del procesador del despachador y parte de la multicolumna NUPI para la tabla.
CollectTimeStamp	Fecha y tiempo único para cada buffer cache, el cual cambia por cada nuevo buffer. Este tiempo se establecerá cuando el cache está listo para recibir un nuevo dato y no cuando las filas son escritas en la base de datos.
QueryID	Identificador generado internamente de la consulta. Este campo se puede combinar con otras tablas DBQL o la tabla DBC.TdwmExceptionLog sin necesidad del campo ProcID.
UserID	Número de identificación único del usuario que ejecuta la consulta que se registra.
AcctString	La cadena de caracteres de la cuenta al momento que

	empezó a ejecutarse la consulta. Las cuentas pueden ser cambiadas dinámicamente a nivel de consulta o sesión.
ExpandAcctString	El nombre de la cuenta extendida bajo la cual la consulta esta ejecutándose si es invocada.
SessionID	Número de identificación único de la sesión
LogicalHostID	Identificador único del origen de inicio de sesión para la consulta registrada. Un valor igual a cero indica una sesión interna.
RequestNum	Número de identificación único de la consulta.
InternalRequestNum	Número de identificación único del pedido interno. Para procedimientos almacenados invocados dentro de una sesión el número de identificación se incrementa en 1 por cada pedido.
LogonDateTime	La estampa del tiempo al empezar la sesión
AcctStringTime	Valor del código de tiempo expandido en la account string. Si el valor no existe, el valor se denota con un “?” y es nulo.
AcctStringHour	Valor del código de hora expandido en la account string. Si el valor no existe, el valor se denota con un “?” y es nulo.
AcctStringDate	Valor del código de fecha expandido en la account string. Si el valor no existe, el valor se denota con un “?” y es nulo.
LogonSource	Texto que representa el origen del inicio de sesión.
AppID	Aplicación (ejecutable) o nombre del utilitario. Por ejemplo: BTEQ
ClientID	Nombre del usuario de red bajo el cual se registra la sesión.
ClientAddr	La dirección IP del cliente que ejecuta la consulta. La misma se obtiene del origen del inicio de sesión desde una red cliente.
QueryBand	La banda de la consulta bajo la cual la consulta se esta

	ejecutando
ProfileID	Nombre del perfil bajo el cual el usuario ejecuta la consulta.
StartTime	La estampa del tiempo cuando se ejecuta la consulta
FirstStepTime	La estampa del tiempo cuando el primer paso se desapacha
FirstRespTime	La estampa del tiempo cuando el primer paquete de respuesta se envia al host
LastStateChange	Tiempo del último cambio de estado para el administrador de carga de Teradata.
NumSteps	Número total de pasos requeridos para el proceso de consulta. Si no se aplica pasos el valor es cero, por ejemplo cuando una consulta es abortada.
NumStepswPar	Número total de pasos incluyendo pasos paralelos
MaxStepsInPar	El máximo número de niveles que se realiza en paralelo para una consulta
NumResultRows	Número total de filas que devuelve una consulta
TotalIOCount	Total de entradas y salidas que utiliza una consulta
AMPCPUTime	Total de tiempo AMP CPU empleado por una consulta
ParserCPUTime	Total de tiempo del Parser y despachador de CPU empleado por una consulta
UtilityByteCount	El número de bytes transferidos por inserción, actualización o eliminación usando Multiload o Fastload
UtilityRowCount	El número de filas insertadas, actualizadas o eliminadas usando Multiload o Fastload
ErrorCode	Número del mensaje de error en ErrorText, si es mayor a cero.
ErrorText	Error de procesamiento y errores del Parser, si no es nulo.
WarningOnly	Indicador si el error fue solamente un warning
DelayTime	El tiempo que una consulta fue demorada por el software de gestión de carga de trabajo en Teradata.
Abort Flag	Si la consulta que empezó a registrarse fue abortada

	podría estar incompleta
CacheFlag	Esta campo esta en blanco si la consulta no se encuentra en el cache. Además puede tener los siguientes valores: “T” si la consulta se encontró en el cache. “S” si la consulta es parametrizada y se genera un plan específico. “G” si la consulta es parametrizada y se genera un plan genérico. “A” si la consulta es parametrizada y se toma una decisión específica.
StatementType	Tipo de la sentencia utilizada en la consulta
QueryText	Los primeros caracteres de la consulta. Por defecto el valor es de 200 caracteres, para ampliar este valor se debe modificar el parámetro LIMIT SQLTEXT
NumOfActiveAmps	Número de AMP activos para la consulta.
MaxAMPCPUTime	Tiempo de CPU, el mas alto valor de CPU utilizado por AMP en la consulta.
MaxCPUAmpNumber	Número de AMP con el valor más alto de actividad de CPU.
MinAmpCPU	Tiempo de CPU, el valor más bajo de CPU utilizado por AMP en una consulta.
MaxAmpIO	Cantidad de entradas y salidas del valor más alto utilizado por AMP en una consulta.
MaxIOAmpNumbe	El número de AMP con la actividad mas alta de entradas y salidas.
MinAmpIO	Cantidad de entradas y salidas, el valor más bajo utilizado por AMP en una consulta.
SpoolUsage	La máxima cantidad de spool usado en el procesamiento de una consulta.
WDID	El número de carga de trabajo asignado a una consulta.
OpEnvID	El identificador interno del entorno operativo reciente

	garantizado por el software de gestión de carga de trabajo de Teradata.
SysConID	El identificador interno del sistema de salud de Teradata
LSN	El número de secuencia de logon usado por la funcionalidad load.
NoClassification	Indica si la consulta no fue clasificada.
WDOverride	Indica si la definición de workload asignada fue anulada.
SLGMet	Indica si la consulta conocida sirvió al nivel de objetivos
ExceptionValue	Valor de la excepción
FinalWDID	Indica la definición del workload para la consulta cuya ejecución se completó.
TDWMEstMaxRows	Cantidad máxima de filas estimada generada por el Optimizador.
TDWMEstLastRows	La última fila estimada generada por el Optimizador.
TDWMEstTotalTime	Tiempo total en segundos estimados por el software de Teradata, basado en el Optimizador, y aplicando las reglas de la base de datos TDWM.
TDWMAllAmpFlag	Indica si una de las etapas de la consulta es un paso total de AMP
TDWMConfLevelUsed	Se completa con la letra “N”.
TDWMRuleID	Identificador de la regla de la consulta.
UserName	Nombre bajo el cual la sesión fue iniciada
DefaultDatabase	Nombre de la base de datos por defecto para la consulta
AMPCPUTimeNorm	Tiempo normalizado de AMP CPU para sistemas coexistentes
ParserCPUTimeNorm	Tiempo normalizado de CPU parceado para sistemas coexistentes
MaxAMPCPUTimeNorm	Número de AMP con el máximo tiempo normalizado de CPU para sistemas coexistentes

MinAmpCPUTimeNorm	Tiempo normalizado mínimo de CPU por AMP.
EstResultRows	Resultado estimado de filas generado por el Optimizador
EstProcTime	Suma del mínimo de tiempo de procesamiento estimado para los pasos en la consulta generado por el Optimizador.
EstMaxRowCount	El número mas grande de filas manejadas por un simple paso en la consulta, según los estima el Optimizador.
StatementGroup	Si una sentencia DDL es solicitada, el StatementGroup reporta con el tipo: • DDL ALTER • DDL CREATE • DDL GRANT Si la sentencia tiene solamente una sentencia DML o múltiples DML del mismo tipo, StatementGroup indica el tipo. Por ejemplo: si hay tres sentencias Delete en una solicitud StatementGroup reporta DML DELETE. En una solicitud de diferentes sentencias DML se mostrará un número de sentencias de cada tipo por solicitud. Por ejemplo, en una solicitud con un insert o dos updates, aparecerían como: DML Del=0 Ins=1 InsSel=0 Upd=2 Sel=0
ProxyUser	El nombre del usuario de la conexión del proxy
ProxyRole	El nombre del rol de la conexión del proxy
WDDelayTime	Los segundos que la consulta fue demorada en la cola del acelerador WD.
ExtraField3	Centésimas de segundos transcurridos en las solicitudes instrumentadas.

Tabla DBQLExplainTbl

Esta tabla se completa si la opción WITH EXPLAIN fue habilitada. Si el texto supera los 64 KB se generan múltiples filas.

El detalle de los campos de la tabla DBQLExplainTBL es la siguiente:

Campo	Descripción
ProcID	Número de identificación único del Despachador y parte de la multicolumna NUPI
CollectTimeStamp	Tiempo en que las filas fueron escritas en la base de datos.
QueryID	Identificador interno generado por la consulta y el FK para otra tabla DBQL.
ExpRowN	Campo utilizado si el texto Explain es mayor a 64 kb y el sistema genera múltiples filas.
ExplainText	Texto completo. El texto no es formateado y aparece como una larga cadena de caracteres.

Tabla DBQLObjTbl

Con la opción WITH OBJECTS, DBQL registra una fila en DBQLObjTbl por cada objeto referenciado en la consulta. Un objeto puede ser una base de datos, una tabla de datos, una columna, un índice secundario, etc.

El detalle de los campos de la tabla DBQLObjTbl es la siguiente:

Campo	Descripción
ProcID	Número de identificación único del Despachador y parte de la multicolumna NUPI
CollectTimeStamp	Tiempo en que las filas fueron escritas en la base de datos.
QueryID	Identificador interno generado por la consulta y el FK para otra tabla DBQL.
ObjectDatabaseName	Nombre de la base de datos que posee el objeto de destino
ObjectTableName	Nombre de la tabla o vista
ObjectColumnName	Nombre de la columna
ObjectID	Número de identificación único del objeto

<table>
<tr><td>ObjectNum</td><td>Número de la columna o índice secundario</td></tr>
<tr><td>ObjectType</td><td>Código de caracteres que representa al objeto

<table>
<tr><td>Tipo de código</td><td>Objeto</td></tr>
<tr><td>Agg</td><td>Función definida agregada por el usuario</td></tr>
<tr><td>AgS</td><td>Función STAT definida agregada por el usuario</td></tr>
<tr><td>Aut</td><td>Autorización de seguridad</td></tr>
<tr><td>Col</td><td>Columna</td></tr>
<tr><td>DB</td><td>Base de datos</td></tr>
<tr><td>Hix</td><td>Indices hasheados</td></tr>
<tr><td>Idx</td><td>Indice. Por cada índice hay un nombre de base de datos, nombre de tabla y nombre de columna.
Para índices de múltiples columnas, hay una fila por cada columna del índice que una consulta utiliza. Por ejemplo, si un índice consiste de tres columnas y la consulta utiliza los tres, serán tres filas cada una con un nombre de columna diferente.</td></tr>
<tr><td>JIx</td><td>Indice Join. Por cada índice join hay un nombre de base de datos y nombre de índice join en el campo del ObjectTableName.</td></tr>
<tr><td>Jrl</td><td>Journal</td></tr>
<tr><td>Mac</td><td>Macro</td></tr>
<tr><td>NoT</td><td>Desconocido (sin tipo)</td></tr>
<tr><td>SP</td><td>Procedimiento almacenado</td></tr>
<tr><td>Sta</td><td>Función STAT</td></tr>
<tr><td>Tab</td><td>Tabla</td></tr>
<tr><td>TbF</td><td>Tabla función</td></tr>
</table></td></tr>
</table>

	Tmp	Temporario
	Trg	Trigger
	UDF	Función definida por el usuario
	UDM	Método definido por el usuario
	UDT	Tipo definido por el usuario
	Viw	Vista
	Vol	Volátil
	XSP	Procedimiento almacenado externo
FreqofUse	Número de veces que el objeto fue accedido, determinado por el Optimizador para procesar la consulta.	
TypeOfUse	Describe el uso del objeto. Contiene los siguientes valores numéricos: 1 = encontrado en la resolución 2 = accedido durante el procesamiento de la consulta. 4 = encontrado en el contexto condicional 8 = encontrado en la condición inner join 16 = encontrado en la condición outer join 32 = encontrado en el nodo de suma 64 = encontrado en una condición full outer join	

Tabla DBQLSQLTbl

Esta tabla se completa si la opción WITH SQL es agregada para la información por defecto. Esta opción causa que DBQL intente registrar la totalidad del texto de la sentencia en la tabla DBQLSQLTbl. Se generan múltiples filas como sea necesario.

El detalle de los campos de la tabla DBQLSQLTbl es la siguiente:

Campo	**Descripción**
ProcID	Número de identificación único del Despachador y parte de la columna múltiple NUPI.
CollectTimeStamp	Tiempo en que las filas fueron escritas en la base de datos.
QueryID	Identificador internamente generado por la consulta.
SQLRowNo	Número de fila de la sentencia

SQLTextInfo	Campo de aproximadamente 32000 caracteres

Si una consulta es abortada el campo SQLTextInfo se puede completar con: Truncated, Null o "Unavailable". La palabra "Unavailable" indica que el sistema no pudo traducir correctamente la sentencia.

Se debe tener en cuenta que, en algunos casos, DBQL no registra la totalidad de la sentencia SQL, por ejemplo: para las sentencias CREATE/REPLACE PROCEDURE se incluyen los argumentos pero no las opciones adicionales ni las sentencias incluidas en el procedimiento almacenado.

Tabla DBQLStepTbl

Esta tabla se completa si se especificó la opción WITH STEPINFO. Cuando la consulta se completa, el sistema registra una fila por cada paso de la consulta, incluyendo los pasos paralelos.

El detalle de los campos de la tabla DBQLSteepTbl es la siguiente:

Campo	Descripción
ProcID	Número de identificación único del Despachador y parte de la columna múltiple NUPI.
CollectTimeStamp	Tiempo en que las filas fueron escritas en la base de datos.
QueryID	Identificador internamente generado por la consulta.
StepLev1Num	Número de paso. Si esta fila es para un paso paralelo, el número se repite.
StepLev2Num	Si esta fila es para un paso paralelo, este es el número de segundo nivel del paso.
StepName	Abreviación de un nombre usado internamente para identificar el paso. Por ejemplo: DEL para un paso DELETE.
StepStartTime	Estampa de tiempo cuando el paso fue enviado al AMP
StepStopTime	Estampa de tiempo cuando el paso retorno del AMP
EstProcTime	Tiempo estimado para el procesamiento determinado por el Optimizador

EstCPUCost	Un tiempo de CPU estimado en milisegundos para el paso determinado por el Optimizador
CPUTime	CPU utilizado por el paso
IOCount	Uso de I/O del paso
EstRowCount	Cantidad de filas estimadas por el Optimizador
RowCount	Si el nombre del paso es MRM (filas múltiples) o EXE (multiload) este campo corresponde al número de filas insertadas. Para todos los otros pasos, el RowCount es el número actual de filas retornadas por el paso.
RowCount2	Si el nombre del paso es MRM (filas múltiples) o EXE (multiload) este campo corresponde al número de filas actualizadas. Si el nombre del paso es LFI (Fastload) RowCount es el número de filas cargadas.
RowCount3	Si el nombre del paso es EXE (multiload) este campo corresponde al número de filas eliminadas
NumofActiveAMPs	El número de AMPs involucrado con el paso
MaxAmpCPUTime	El máximo tiempo de CPU utilizado de AMP en el paso
MaxCPUAmpNumber	El número de AMP con el máximo CPU utilizado por el paso
MinAmpCPUTime	El mínimo tiempo de CPU utilizado de AMP en el paso
MaxAmpIO	Cantidad de I/O del mas alto I/O utilizado de AMP en el paso
MaxIOAmpNumber	El número de AMP con el mas alto uso de I/O para el paso
MinAmpIO	Cantidad de I/O del menor I/O de AMP utilizado en la consulta
SpoolUsage	El número de bytes de spool utilizado por el paso
MaxAMPSpool	El mas alto uso de spool sobre un AMP
MaxSpoolAmpNumber	Número de AMP con un alto uso de spool
MinAMPSpool	El mas bajo uso de spool sobre un AMP
StepWD	La definición de workload en efecto para el paso

LSN	El número de secuencia de logon utilizado por la utilidad load
UtilityTableId	El número de identificación de la tabla para la utilidad Este campo es siempre cero
RowsWComprColumns	Número de filas con filas comprimidas
EstIOCost	Un tiempo estimado de servicio en milisegundos para la I/O del paso.. No hay un dato actual para este campo
EstNetCost	Un tiempo estimado de BYNET del tiempo de servicio en milisegundos para el paso. No hay un dato actual para este campo
EstHRCost	Un estimado de otros costos para el paso. No hay un dato actual para este campo
CPUTimeNorm	Tiempo AMP CPU normalizado para sistemas coexistentes
MaxAmpCPUTimeNorm	Tiempo máximo de CPU normalizado por AMP
MaxCPUAmpNumberNorm	Número de AMP con el tiempo máximo normalizado de CPU para sistemas co-existentes
MinAmpCPUTimeNorm	Tiempo mínimo de CPU normalizado por AMP

Los pasos reflejados en DBQLStepTbl son generados por la base de datos de Teradata para ejecutar una consulta. Ellos pueden no siempre coincidir con pasos que se muestran en el Explain porque algunos pasos son de uso interno únicamente.

En la siguiente tabla se describen los nombres de los pasos registrados y su significado:

Nombre interno del paso	**Descripción**
AAB	Aborto asincrónico de un pedido DBC/SQL
ALT	Agrega un número de identificación de tabla en el segmento HUT de control para el número de secuencia de inicio de sesión
AltGrp	Cambia el grupo de replicación
BMSMS	Mapea bit para manipular una intersección y una unión

CIX	Crea un índice secundario
CkNPK	Verifica N claves padres
CKP	Punto de verificación de la base de datos
CRI	Creación de un índice de referencia
CrtGrp	Creación de un grupo de replicación
CSSUM	Recolecta estadísticas de operaciones globales
CSUPD	Recolecta estadísticas actualizadas
Ctb	Creación de la cabecera de una tabla
CTRts	Creación de privilegios de una tabla
DEL	Eliminación de filas
DELQT	Eliminación de filas desde una cola de tabla
DIRI	Borra inconsistencia de índices referenciales
DIX	Eliminación de índices secundarios
DJT	Eliminación de tabla diaria
DRI	Eliminación de índice de referencia
DRIDR	Eliminación de filas RID
DrpGrp	Borra un grupo de replicación
DTB	Borra una tabla
DTmp	Elimina tablas temporales
EBD	BEGIN EDIT DELETE
EBE	BEGIN MLOAD
EDM	Prepara para desbloquear una tarea o una aplicación
Edt	Fin de transacción
EED	Prepara tablas de trabajo MLOAD
EEN	Fin de la edición de pasos
ERE	Libera las tablas de trabajo MLOAD
ESD	Adquisición de datos
ESR	Ordena las tablas de trabajo MLOAD
EVT	Creación una fila de una tabla de eventos
EXE	Ejecución de la edición
ExecSP	Ejecución de procedimientos almacenados
ExpHR	Exportación de paso de redistribución horizontal
ExpRL	Exportación de liberación de pasos bloqueados

ExpVR	Exportación vertical de paso de redistribución
Fail	Operación que no opero
FCF	Configuración de frente
FDS	Entrada de la tabla de contabilidad dbspace Flush
FLGRI	Bandera del índice de referencia
Hcs	Agrega un registro de información y privilegios a la tabla en el segmento del Hut Control para un número de secuencia de inicio de sesión.
HLA	Acceso de alto nivel a un objeto
HUL	Utilidad del host par bloqueo
ILR	Contiene entrada a los accesos de logs
INS	Inserción de una fila
INSLDC	Inserción de un Lob Constante diferida
INSQT	Inserción de una fila a una tabla de cola
InvJHI	Invalido Join con el hash del índice
JIN	Join
JTmp	Tablas temporales diarias
LBG	Inicio de la carga de datos
LCM	Carga de mapeo de configuración
LCP	Punto de control de la carga de datos
LFI	Fin de carga de datos
LIN	Uso de insert en la carga de datos
LobFet	Objeto grande de extracción
LogAOf	Registro para archivos apagados en línea
LogAOn	Registro para archivos encendidos en línea
LOT	Objeto grande de transporte
LOT2VM	Envio de un LOT a un mailbox virtual
MDT	Unión de tablas borradas
MiIns	Unión interna de insert
MiRet	Unión interna de retrieve
MiUpd	Unión interna de update
MLK	Múltiple bloqueo
MRD	Unión de dos tablas borradas basadas sobre el código de hash

	de fila
MRG	Unión de dos tablas basadas sobre el código de hash de fila
MRL	Unión de utilidad de bloqueo
MRU	Unión de update
MRM	Unión de operaciones de filas múltiple
MTB	Modificación de tabla
MTH	Modificación del encabezado (header) de una tabla
MTmp	Materializar tablas temporales
MVN	Modificación del número de versión del encabezado (header) de una tabla
NEXTOK	Es la confirmación para continuar al próximo paso
OAR	Un respuesta de un AMP
Okay	Operación realizada
OKELCT	Envia el mensaje StpOKElicitData para notificar al Despachador que esta disponible para enviar el próximo paso dentro del mismo pedido.
PFN	Proceso de función
PKA	Primer rechazo de clave
PRELOB	Paso InsPreLob
QryLgn	Inicio de sesión de la consulta en el paso
RAE	Remueva la entrada de rechazo desde la lista TOABORT
RepPh1	Paso de la replicación en la fase 1
RepRCR	Repetición de la replicación del mensaje de filas cambiadas
RET	Filas retiradas
RpChg	Suscripción de la replicación del mensaje de filas cambiadas
RSF	Liberación de archivos en spool
SAMP	Realiza el muestreo desde la tabla
SAT	Sincroniza pasos de pruebas rechazados desde las sentencias DBC / SQL
SMS	Conjunto de manipulaciones tales como intersección, unión y exclusión
SplDB	Deterioro de la información de la base de datos en el diccionario de datos

SpIPSC	Deterioro de la información de la sesión del Analizador
SpIQL	Deterioro de la regla DBQL en cache
SpIRTS	Deterioro de la información en cache del procedimiento almacenado
SpITAB	Deterioro de la información de la tabla en el diccionario de datos
SQB	Conjunto de Query_Band
SQL	Paso SQL para el pedido de almacenamiento de texto
SRD	Ordenar una tabla
STATFN	Realizar funciones estadísticas
StpRLK	Liberar bloqueo
SUM	Realizar agregados locales de operaciones
TRET	Trigger recuperado
UPD	Actualización de fila
UpsIns	Upsert insert
UpsUpd	Upsert update
VJT	Validar la tabla diaria
Warn	Respuesta de advertencia

Tabla DBQLSummaryTbl

Esta tabla se completa si se seleccionó la opción “Summary” o la opción “Threshold”.

Si se utiliza “Threshold” se registran las consultas menores o iguales al criterio definido. Dicho criterio puede ser: segundos transcurridos, tiempo normalizado, cantidad de entradas/salidas, centésimas transcurridas, AMP CPU o centésimas de segundos.

Las consultas que superan el umbral se registran en la tabla DBQLogTbl

El empleo de la opción “Summary” tiene las siguientes características:

- No se generan filas por defecto en la tabla DBQLogTbl.
- Al definir un criterio las consultas se agrupan en cubos. Cada cubo cuenta el número de consultas por sesión y suma el tiempo transcurrido, cantidad de entradas y salidas y tiempos de CPU.
- El contenido de la tabla es confirmado cada 10 minutos cuando se vacía el cache.

El detalle de los campos de la tabla DBQLSummaryTbl es el siguiente:

Campo	Descripción
ProcID	Número de identificación único del Despachador y parte de la columna múltiple NUPI.
CollectTimeStamp	Tiempo en que las filas fueron escritas en la base de datos.
UserID	Número de identificación único del usuario cuya consulta se registra.
AcctString	El nombre de la cuenta no expandida bajo la cual la consulta se ejecuta.
LogicalHostID	Número de identificación único del origen del inicio de sesión de la consulta registrada. El valor cero indica una sesión interna.
AppID	Número de identificación único de la aplicación bajo la cual la consulta se ejecuta.
ClientID	Número de identificación del cliente bajo el cual la consulta se ejecuta
ClientAddr	Número de dirección ip del cliente bajo el cual la consulta se ejecuta
ProfileID	Número de identificación del perfil bajo el cual el usuario ejecuta la consulta
SessionID	Número de identificación de la sesión en la cual se empezó a ejecutar la consulta.
QueryCount	Número de consultas que se ejecutaron los últimos 10 minutos
ValueType	El criterio del umbral es el siguiente: • C = segundos AMP CPU • H = centésimas de segundo transcurridos • I = cantidad de entradas/ salidas • N = segundos de AMP CPU normalizados • S = tiempo en segundos transcurridos.
QuerySeconds	Total del tiempo de ejecución de la consulta en un periodo para el histograma.

	Calculado en el valos mas próximos en centésimas de segundo.
TotalIOCount	Cantidad total de entradas y salidas
AMPCPUTime	Tiempo total de AMP CPU
ParserCPUTime	Tiempo de AMP CPU normalizado para sistemas coexistentes únicamente.
ParserCPUTimeNorm	Tiempo de CPU normalizado para el análisis de las consultas
HighHist	El valor mas alto para la opción SUMMARY Cero para la opción THRESHOLD. Si los modificadores CPUTIME or IOCOUNT son utilizados luego este valor es el mas alto entre segundos en CPU o cantidad de entradas y salidas por usuario.
LowHist	El menor valor para la opción SUMMARY Para la opción THRESHOLD el valor es el tiempo de umbral configurado para el usuario. El tiempo por defecto es 5. Si los modificadores CPUTIME or IOCOUNT son utilizados luego este valor es el menor entre segundos en CPU o cantidad de entradas y salidas por usuario.

Tabla DBQLXMLTbl

Esta tabla se completa si la opción WITH XMLPLAN fue seleccionada en la sentencia BEGIN QUERY LOGGING o REPLACE QUERY LOGGING. El detalle de los campos de la tabla DBQLXMLTbl es el siguiente:

Campo	**Descripción**
ProcID	Número de identificación único del Despachador y parte de la columna múltiple NUPI.
CollectTimeStamp	Tiempo en que las filas fueron escritas en la base de datos.
QueryID	Identificador único generado internamente para la

	consulta.
XMLRowNo	Número en una secuencia de las filas que constituyen un plan
XMLTextInfo	Plan XML Si el plan XML es muy grande es guardado en una o mas filas cada una de las cuales contiene un subconjunto del plan.

Se acota que la opción WITH ALL no registra el plan de la consulta a la tabla DBQLXMLTbl.

Anexo III: Gestión de tablas temporales e históricas DBQL de Teradata

Tratamiento de las tablas temporales DBQL y tablas históricas DBQL.
En forma diaria deben realizarse los siguientes pasos

Paso 1

- Verificar que DBQLOGTBL_TMP, DBQLSQLTBL_TMP, DBQLOBJTBL_TMP and DBQLSummaryTBL_TMP se encuentran vacías.
- Ejecutar la sentencia END QUERY LOGGING sobre el ID de un usuario para vaciar los buffers.
- Ejecutar el macro SYS_MGMT.LoadDBQLTMP. Este macro levanta las tablas temporales DBQL desde las tablas DBC DBQL y elimina los datos desde las tablas DBC DBQL.
- Ejecutar la sentencia BEGIN QUERY LOGGING sobre el ID de un usuario para el cual el registro se ha finalizado.
- Ejecutar la sentencia COLLECT STATISTICS sobre las tablas temporales DBQL

Paso 2

- Verificar que las tablas temporales DBQL tienen filas.
- Ejecutar el macro SYS_MGMT.LoadDBQLHSTTBLS. Este macro levanta DBQLOGTBL_HST, DBQLSQLTBL_HST, DBQLOBJTBL_HST, DBQLOBJTBL_SUM y DBQLSummaryTBL_HST y elimina los datos desde las tablas temporales DBQL.
- Ejecutar la sentencia COLLECT STATISTICS sobre DBQLOGTBL_HST, DBQLSQLTBL_HST, DBQLOBJTBL_HST, DBQLOBJTBL_SUM y DBQLSummaryTBL_HST

Mensualmente el proceso de mantenimiento consiste en un ejecutar el macro SYS_MGMT.PRGDBQLHSTTBLS.

Se recomienda conservar los datos por un periodo de un año para realizar búsquedas de datos.

Anexo IV: Detalle de la vista DBC.DBQLRulesV de Teradata

Vista DBC.DBQLRulesV

Campo	Descripción
User name	Nombre del usuario para el que se definieron las reglas de registro.
Account	Cuenta para la cual se definieron las reglas de registro o la que se definió como calificador para registrar sesiones de un usuario.
ApplicationNam	Nombre de la aplicación para la que se definieron las reglas de registro.
TypeOfRule	Indica si hay una regla que se inhabilito su registro para el usuario, cuenta o aplicación.
WITH logging option flags (si esta definida)	Cualquier opción de registro WITH definida para un usuario o cuenta, tales como OBJECT, EXPLAIN, STEPINFO, SQL, SQLTEXT, SUMMARY, THRESHOLD, o XMLPLAN.
LIMIT logging option flags (si esta definida)	Cualquier opción de registro LIMIT definida para un usuario o cuenta
TextSize	Número de bytes del texto en el campo QueryText de la tabla DBQLogTbl
TypeOfCriterion	Especifica uno de los siguientes criterios con las opciones de summary o treshold: • ElapsedSec: segundos transcurridos • CPUTime: tiempo en CPU (centésimas de segundos) • IOCount: cantidad de entradas y salidas • CPUTimeNorm: tiempo normalizado de CPU (centésimas de segundos) para sistemas coexistentes • ElapsedTime: tiempo transcurrido (centésimas de segundos)

	• No criteria: ningún criterio

Anexo V: Ejemplo de procedimiento threshold de Teradata

Ejemplo de procedimiento treshold

```
declare @audit_table_number int
/*
** Select the value of the current audit table
*/
select @audit_table_number = scc.value
from master.dbo.syscurconfigs scc, master.dbo.sysconfigures sc
where sc.config=scc.config and sc.name  = “current audit table”
/* Set the next audit table to be current.
** When the next audit table is specified as 0,
** the value is automatically set to the next one.*/
exec sp_configure “current audit table”, 0, “with truncate”
/*** Copy the audit records from the audit table
** that became full into another table.*/
if @audit_table_number = 1
   begin
      insert aud_db.sso_user.sysaudits
         select * from sysaudits_01
      truncate table sysaudits_01
   end
else if @audit_table_number = 2
   begin
      insert aud_db.sso_user.sysaudits
         select * from sysaudits_02
      truncate table sysaudits_02
   end
return(0)
```

Anexo VI: Opciones de auditoria de SAP Adaptive Server Enterprise

Variantes de option del comando sp_audit

Valor	Descripción
Adhoc	Los usuarios autorizados pueden emplear sp_addauditrecord para agregar sus propios registros a la auditoria.
All	Todas las acciones realizadas por un usuario particular o por los usuarios de un rol particular. Esta opción solo se puede aplicar a roles del sistema.
Alter	Audita la ejecución de los comandos alter table o alter database.
Bcp	Audita la ejecución de la utilidad bcp.
Bind	Audita la ejecución de los procedimientos almacenados del sistema sp_bindefault, sp_bindmsg y sp_bindrule
Cmdtext	Audita todos los comandos escritos por un usuario en particular.
Create	Audita la creación de objetos de bases de datos.
Dbaccess	Audita el acceso a una base de datos actual desde otra base de datos.
Dic	Audita la ejecución de cualquier comando dbcc
Delete	Audita la eliminación de filas desde una tabla o vista.
Disk	Audita la ejecución de disk init, disk refit, disk reinit, disk mirror, disk unmirror y disk remirror.
Drop	Audita la eliminación de objetos de la base de datos
Dump	Audita la ejecución de dump database o dump transaction.
Encryption_key	Audita la creación, modificación y eliminación de la clave de cifrado y ejecución de sp_encryption.
Errors	Audita errores, sean fatales o no.
Errorlog	Audita la ejecución de sp_errorlog o la función errorlog_admin
Exec_procedure	Audita la ejecución de un procedimiento almacenado.

Exec_trigger	Audita la ejecución de un trigger.
Func_dbaccess	Audita el acceso a una base de datos a través de una función de Transact-SQL
Func_obj_access	Audita el acceso a un objeto de una base de datos a través de una función de Transact-SQL.
Grant	Audita la ejecución del comando grant
Insert	Audita la inserción de filas a una tabla o vista.
Install	Audita la instalación de clases de Java
Load	Audita la ejecución del comando load database o load transaction
Login	Audita todos los intentos de inicio de sesión en el motor de base de datos.
Login_locked	Audita los logins que se bloquean porque superaron el número de intentos fallidos establecido.
Logout	Audita todos los cierres de sesión en el motor de base de datos.
Mount	Audita los comandos mount database.
Password	Audita los cambios en la política de contraseñas.
Quiesce	Audita los comandos quiesce database.
Referente	Audita referencias entre tablas.
Remove	Audita la remoción de clases de Java.
Revoke	Audita la ejecución del comando revoke.
Rpc	Audita la ejecución de llamadas a procedimientos remotos.
Security	Audita los siguientes eventos de seguridad Encendido y apagado de un servidor Activación y desactivación de un rol Ejecución de alguno de los siguientes comandos: • addcert • connect • create and drop login • dropcert • create, drop, alter, grant, and revoke role

	• kill • online database • set proxy • set session authorization • sp_configure Ejecución de alguna de las siguientes funciones: • config_admin • set_password • valid_user • attr_notify • ha_add_companion • ha_remove_companion • ha_check_alive • ha_getversion • ha_failback • ha_retrestrictionclass • ha_getrcs • ha_setrcs • ha_hacluster_verify • js_wakeup • unlock_admin_account • ssl_admin • ws_admin • valid_user • proc_role (desde dentro de un procedimiento de sistema) Regeneración de claves SSO
Select	Audita la ejecución de la sentencia select.
Setuser	Audita la ejecución de la sentencia setuser.
Sproc_auth	Audita las verificaciones de autorizaciones que se encuentran dentro de los procedimientos almacenados.
Table_access	Audita el acceso a cualquier tabla por un usuario

	específico.
Transfer_table	Audita transferencia entre tablas. Esta opción no se encuentra en la tabla sysauditoptions.
Truncate	Audita la ejecución de la sentencia truncate table
Unbind	Audita la ejecución de sp_unbindrule, sp_unbindmsg, y sp_unbindefault.
Unmount	Audita la ejecución del comando umount database
Update	Audita actualización de filas en una tabla o una vista
View_access	Audita los accesos a una vista por un usuario específico

Anexo VII: Detalle de sysaudits y sybsecurity de SAP Adaptive Server Enterprise

Composición de la tabla sysaudits

Nombre de la columna	Tipo de datos	Descripción
event	smallint	Tipo de evento que se registro. Al final del presente anexo se detallan los distintos eventos.
eventmod	smallint	Brinda mayor información sobre el evento que se registra. Los valores posibles son: 0 = no hay modificador para este evento. 1 = el evento paso la verificación de permisos. 2 = el evento no paso la verificación de permisos
spid	smallint	Número de identificación del proceso que causo que se registre el evento
eventtime	datetime	Fecha y hora de ocurrencia del evento.
sequence	smallint	Número de secuencia del registro dentro de un evento. Algunos eventos requieren mas de una fila o registro.
suid	smallint	Número de identificación del login del usuario que realizó el evento
dbid	int null	Número de identificación de la base de datos en la cual ocurrió el evento o en la cual el objeto, procedimiento almacenado o trigger reside, esto depende del tipo de evento.
objid	int null	Número de identificación del objeto, procedimiento almacenado o trigger al que se accedió.
xactid	binary(6) null	Número de identificación de la transacción del evento registrado. Para una transacción de múltiples bases de datos, se considera el

		número de identificación de la transacción de la base de datos de origen.
loginname	varchar(30) null	Nombre del login correspondiente al suid.
dbname	varchar(30) null	Nombre de la base de datos correspondiente al dbid.
objname	varchar(30) null	Nombre del objeto correspondiente al objid.
objowner	varchar(30) null	Nombre del dueño del objid.
Extrainfo	varchar(255) null	Información adicional del evento registrado. Esta columna contiene una secuencia de los ítems separado por comas. Al final del presente anexo se presenta mayor detalle de este campo.
Nodeid	tinyint	Número de identificación del nodo del servidor en el cluster donde el evento ocurrió.

Detalle de los eventos registrados en sybsecurity

Nro. de evento	Comando	Nro. de evento	Comando
1	ad hoc audit record	56	Reserved
2	alter database	57	Reserved
3	alter table	58	Reserved
4	bcp in	59	Reserved
5	Reserved	60	Reserved
6	bind default	61	access to audit table
7	bind message	62	select table
8	bind rule	63	select view
9	create database	64	truncate table
10	create table	65	Reserved
11	create procedure	66	Reserved
12	create trigger	67	unbind default
13	create rule	68	unbind rule
14	create default	69	unbind message
15	create message	70	update table
16	create view	71	update view
17	access to database	72	Reserved
18	delete table	73	auditing enabled
19	delete view	74	auditing disabled
20	disk init	75	Reserved
21	disk refit	76	SSO changed password
22	disk reinit	77	Reserved
23	disk mirror	78	Reserved

24	disk unmirror	79	Reserved
25	disk remirror	80	role check performed
26	drop database	81	dbcc
27	drop table	82	config
28	drop procedure	83	online database
29	drop trigger	84	setuser command
30	drop rule	85	UDR command
31	drop default	86	built-in function
32	drop message	87	Disk release
33	drop view	88	set SSA command
34	dump database	89	kill or terminate command
35	dump transaction	90	connect
36	Fatal error	91	reference
37	Non-fatal error	92	command text
38	execution of stored procedure	93	JCS install command
39	Execution of trigger	94	JCS remove command
40	grant	95	Unlock admin account
41	insert table	96	quiesce database
42	insert view	97	create SQLJ function
43	load database	98	drop SQLJ function

44	load transaction	99	SSL administration
45	login	100	disk resize
46	logout	101	mount database
47	revoke	102	unmount database
48	rpc in	103	login command
49	rpc out	104	create index
50	server boot	105	drop index
51	server shutdown	106	Reserved
52	Reserved	107	Reserved
53	Reserved	108	Reserved
54	Reserved	109	Reserved
55	role toggling	110 111	deploy user-defined web services undeploy user defined web services
112	Login locked due to exceeding the configured number of failed attempts	113	quiesce database..hold security
114	quiesce database..release	115	sp_passwordpolicy and all of its actions except "list"
116	create manifest file	117	Regeneration of asymmetric keypairs for network password encryption by system or sp_passwordpolicy
118	alter encryption key modify encryption	119	alter encryption key add encryption

120	alter encryption key drop encryption	121	Reserved
122	alter encryption key recover encryption	123	LDAP state changes
124	Cluster commands	125	When sp_passwordpolicy 'set', 'disalow simple passwords', 1, and a login with a simple password is created using create login.
126	Reserved	127	Errorlog administration with sp_errorlog
128	Reserved	129	Reserved
130	Reserved	131	Reserved
132	alter...modify owner	133	alter role..lock
134	alter role..add passwd alter role..drop passwd create role..with passwd	135	alter encryption key..regenerate key
136	transfer table	137	create login profile
138	alter login	139	drop login
140	alter login profile	141	drop login profile
142	create thread pool	143	alter thread pool
144	drop thread pool	145	sp_hidetext
146	sproc_auth	147	Reserved
148	Reserved	149	dump configuration to

150	dump database..cumulative to	151	load database..cumulative from
152	Reserved	153	Reserved
154	Configuration history	155	alter index
156	----	157	Reserved
158	Reserved	159	Reserved

Detalle del contenido de la columna extrainfo

Posición	Categoría	Descripción
1	Roles	Una lista de roles activos, separados por comas
2	Palabras claves u opciones	El nombre de la palabra clave u opción que fue usado en el evento. Si hay múltiples palabras claves u opciones son listadas separadas con comas.
3	Valor previo	Si el evento es la actualización de un valor, este item contiene el valor anterior a la ejecución del comando update.
4	Valor actual	Si el evento es la actualización de un valor, este item contiene el nuevo valor correspondiente a la ejecución del comando update.
5	Otra información	Información adicional relativa a seguridad que es registrada para el evento.
6	Información de proxy	El nombre del login original si el evento ocurre mientras se utiliza un set proxy.
7	Nombre Principal	El nombre principal del login del usuario.

Por ejemplo: un cambio en un parámetro de configuración de la auditoria se podría observar en la columna extrainfo de la siguiente manera:

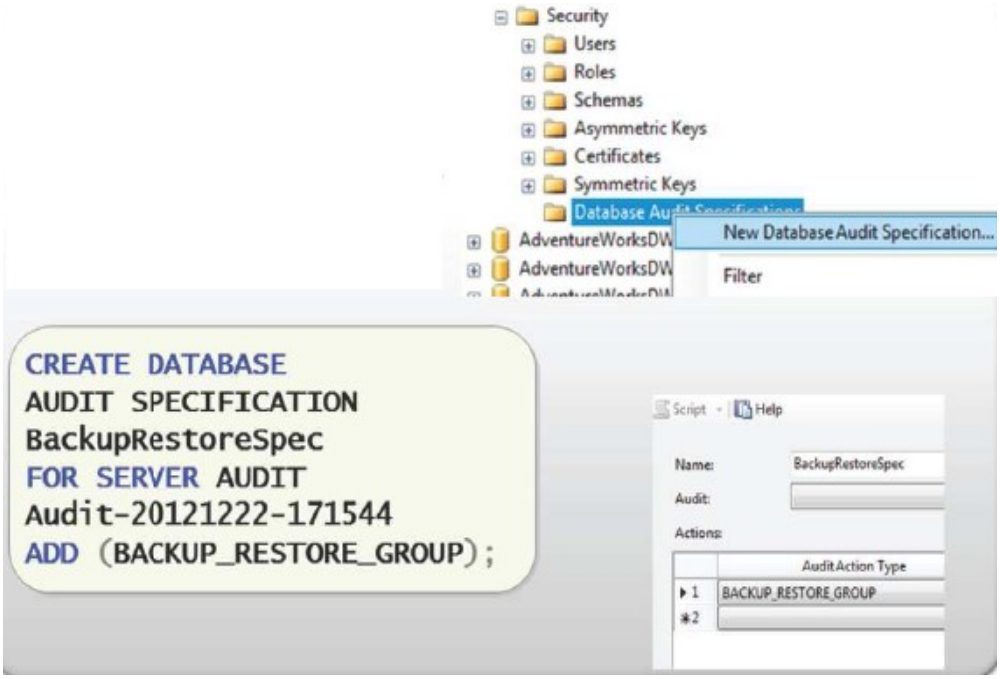
sso_role;suspend audit when device full;1;0;;Ralph;

En la misma se observa que el usuario Ralph estaba operando con un proxy login. No se provee el nombre principal. Dicho usuario que tiene el rol SSO cambio el parámetro suspend audit when device full del valor 1 a 0.

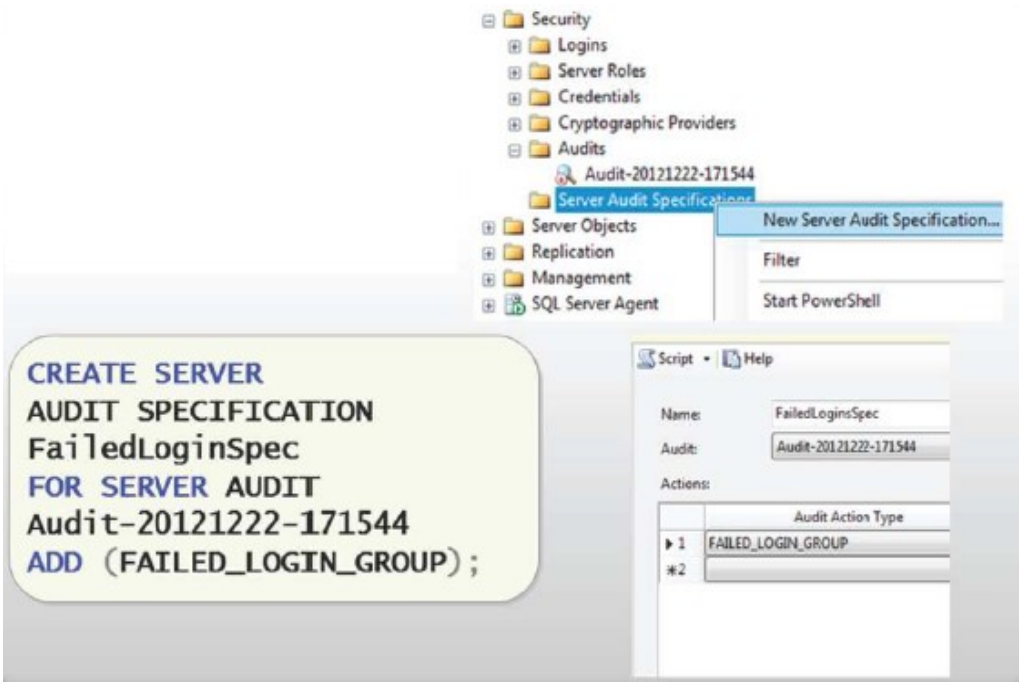
Anexo VIII: Ejemplos de SQL AUDIT de Sql Server

Ejemplos de la funcionalidad SQL AUDIT

- A nivel de base de datos, el nombre de la especificación es BackupRestoreSpec y los datos colectados se envían a la auditoría Audit-20121222-171544. El action group a ser auditado es el BACKUP_RESTORE_GROUP



- A nivel de servidor, el nombre de la especificación es FailedLoginSpec y los datos colectados se envían a la auditoría Audit-20121222-171544. El action group a ser auditado es el FAILED_LOGIN _GROUP



Anexo IX: Detalle de los ACTIONS GROUP de Sql Server

Actions group	Descripción
AUDIT_CHANGE_GROUP	Todos los cambios realizados en una auditoría se auditan en ella.
BACKUP_RESTORE_GROUP	Este evento tiene lugar cuando se emite un comando de copia de seguridad o de restauración.
DATABASE_CHANGE_GROUP	Este evento se desencadena al crear, modificar o quitar una base de datos.
DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP	Este evento se provoca para cualquier cambio de propiedad de objetos en cualquier base de datos del servidor.
APPLICATION_ROLE_CHANGE_PASSWORD_GROUP	Este evento se desencadena cuando se cambia una contraseña para un rol de aplicación.
DATABASE_OBJECT_PERMISSION_CHANGE_GROUP	Este evento se desencadena al emitir una instrucción GRANT, REVOKE o DENY para los objetos de bases de datos, como los ensamblados y los esquemas. Este evento se desencadena para cualquier cambio de permisos de objetos en cualquier base de datos del servidor.
DATABASE_PRINCIPAL_CHANGE_GROUP	Este evento se provoca al crear, modificar o quitar entidades de seguridad, como usuarios, en una base de datos.
DATABASE_PRINCIPAL_IMPERSONATION_GROUP	Este evento se desencadena cuando hay una suplantación en el ámbito de la base de datos, por ejemplo, EXECUTE AS <principal> o SETPRINCIPAL. Este evento se desencadena para las suplantaciones realizadas en cualquier base de datos.
DATABASE_ROLE_MEMBER_	Este evento se desencadena cuando se

CHANGE_GROUP	agrega o se quita un inicio de sesión en un rol de base de datos. Esta clase de eventos se desencadena para los procedimientos almacenados sp_addrolemember, sp_changegroup y sp_droprolemember.
DBCC_GROUP	Este evento se desencadena cuando una entidad de seguridad emite un comando DBCC.
FAILED_LOGIN_GROUP	Indica que una entidad de seguridad intentó iniciar una sesión de SQL Server, pero no lo consiguió. Los eventos de esta clase los producen nuevas conexiones o conexiones reutilizadas de un grupo de conexiones.
LOGIN_CHANGE_PASSWORD_GROUP	Este evento se produce cuando se cambia una contraseña de inicio de sesión mediante la instrucción ALTER LOGIN o el procedimiento almacenado sp_password.
LOGOUT_GROUP	Indica que una entidad de seguridad ha finalizado una sesión de SQL Server. Los eventos de esta clase los producen nuevas conexiones o conexiones reutilizadas de un grupo de conexiones.
SCHEMA_OBJECT_CHANGE_GROUP	Este evento se desencadena al realizar una operación CREATE, ALTER o DROP en un esquema.
SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP	Este evento se desencadena al realizar una operación de concesión, denegación o revocación en un objeto de esquema.
SERVER_OBJECT_CHANGE_GROUP	Este evento se desencadena con las operaciones CREATE, ALTER o DROP en objetos de servidor.

SERVER_OBJECT_OWNERSHIP_CHANGE_GROUP	Este evento se desencadena al cambiar el propietario de los objetos en el ámbito del servidor.
SERVER_OBJECT_PERMISSION_CHANGE_GROUP	Este evento se desencadena cuando una entidad de seguridad de SQL Server emite una instrucción GRANT, REVOKE o DENY para un permiso de objeto de servidor.
SERVER_OPERATION_GROUP	Este evento se desencadena al usar operaciones de auditoría de seguridad, como la modificación de la configuración, los recursos, el acceso externo o la autorización.
SERVER_PRINCIPAL_CHANGE_GROUP	Este evento se desencadena al crear, modificar o quitar entidades de seguridad de servidor. Este evento se desencadena cuando una entidad de seguridad emite los procedimientos almacenados p_defaultdb o sp_defaultlanguage o instrucciones ALTER LOGIN. Este evento se desencadena en los procedimientos almacenados sp_addlogin y sp_droplogin. Este evento se desencadena para los procedimientos almacenados sp_grantlogin, sp_revokelogin o sp_denylogin. Equivalente a Audit Login GDR (HYPERLINK "http://msdn.microsoft.com/es-es/library/ms190740.aspx"claseHYPERLINK "http://msdn.microsoft.com/es-es/library/ms190740.aspx" de HYPERLINK "http://msdn.microsoft.com/es-es/library/ms190740.aspx"eventosHYPERLINK "http://msdn.microsoft.com/es-

	es/library/ms190740.aspx").
SERVER_PRINCIPAL_IMPERSONATION_GROUP	Este evento se desencadena cuando hay una suplantación en el ámbito del servidor, como EXECUTE AS <inicioDeSesión>.
SERVER_ROLE_MEMBER_CHANGE_GROUP	Este evento se desencadena cuando se agrega o quita un inicio de sesión en un rol fijo de servidor. Este evento se desencadena para los procedimientos almacenados sp_addsrvrolemember y sp_dropsrvrolemember.
SERVER_STATE_CHANGE_GROUP	Este evento se desencadena al modificar el estado del servicio de SQL Server.
SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP	Indica que una entidad de seguridad inició una sesión correctamente en una base de datos independiente. Equivalente a la clase de eventos de auditoría correcta de autenticación de base de datos.
SUCCESSFUL_LOGIN_GROUP	Indica que una entidad de seguridad ha iniciado correctamente una sesión de SQL Server. Los eventos de esta clase los producen nuevas conexiones o conexiones reutilizadas de un grupo de conexiones.
USER_CHANGE_PASSWORD_GROUP	Este evento se desencadena cuando la contraseña del usuario de una base de datos independiente se cambia utilizando la instrucción ALTER USER.
USER_DEFINED_AUDIT_GROUP	Este grupo supervisa los eventos producidos utilizando sp_audit_writeHYPERLINK "http://msdn.microsoft.com/es-es/library/gg471540.aspx" (HYPERLINK "http://msdn.microsoft.com/es-es/library/gg471540.aspx"TransactHYPER

	LINK "http://msdn.microsoft.com/es-es/library/gg471540.aspx"-SQL). Normalmente, los desencadenadores o los procedimientos almacenados incluyen llamadas a sp_audit_write para habilitar la auditoría de eventos importantes.
FAILED_DATABASE_AUTHENTICATION_GROUP	Indica que una entidad de seguridad intentó iniciar una sesión en una base de datos independiente y no pudo conseguirlo. Los eventos de esta clase los producen nuevas conexiones o conexiones reutilizadas de un grupo de conexiones.

Anexo X: Contenido de los archivos de extensión trc de Sql Server

Nombre de la columna	Número de la columna	Descripción
Application Name	10	Nombre de la aplicación cliente que creo la conexión a una instancia de SQL Server.
Binary Data	2	Valor binario que depende del evento de la clase capturado en la traza de auditoría.
ClientProcessID	9	Número de identificación asignado por la computadora al proceso donde la aplicación del cliente se ejecuta.
Column Permissions	44	Indica si un permiso sobre una columna fue establecido.
CPU	18	Cantidad de tiempo de cpu, en milisegundos usados por el evento.
Database ID	3	Número de identificación de la base de datos especificada en la sentencia USE o la base de datos por defecto si la sentencia USE no se ha emitido.
DatabaseName	35	Nombre de la base de datos en la cual la sentencia del usuario está ejecutándose.
DBUserName	40	Nombre del usuario de SQL Server del cliente.
Duration	13	Cantidad de tiempo, en milisegundos tomados por el evento.
End Time	15	Tiempo en el cual el evento finalizó. Esta columna no se completa para los eventos de clases que se refieren a eventos de inicio, tales como SQL:BatchStarting o SP:Starting
Error	31	Número de error de un evento dado. Generalmente este es el número de error guardado en sysmessages

EventClass	27	Tipo de la clase del evento capturado.
EventSubClass	21	Tipo de la subclase del evento, provee información adicional de cada clase de evento.
FileName	36	Nombre lógico del archivo que empezó a modificarse.
Andel	33	Número entero usado por ODBC, OLE DB, o DB-Library para coordinar la ejecución del servidor.
Host Name	8	Nombre de la computadora sobre la cual el cliente esta corriendo.
Index ID	24	Número de identificación del índice sobre el objeto afectado por el evento.
Integer Data	25	Número entero dependiente de la clase de evento capturado en la traza.
LoginName	11	Nombre del login del usuario (login de SQL Server o las credenciales de Microsoft Windows en el formato Domain\nombre del usuario.
LoginSid	41	Número de identificación de seguridad (SID) del usuario logeado. Este dato se puede encontrar en la tabla syslogins de la base de datos master. Cada SID es único por cada login en el servidor.
Mode	32	Número entero usado por varios eventos que describen un estado del evento que se recibió o se solicitó.
NestLevel	29	Número entero que representa el dato retornado por @@NESTLEVEL.
NT Domain Name	7	Dominio de Microsoft Windows NT® 4.0 o Windows 2000 al que el usuario pertenece.
NT User Name	6	Nombre del usuario de Windows NT 4.0 o

		Windows 2000.
Object ID	22	Número de identificación asignado al objeto.
ObjectName	34	Nombre del objeto que se empezó a referenciar.
ObjectType	28	Valor que representa el tipo de objeto involucrado en el evento. Este valor corresponde a la columna type en sysobjects.
Owner Name	37	Nombre del propietario de la base de datos.
Permissions	19	Número entero que representa el tipo de permiso verificado. Los valores posibles son:
		1 = SELECT ALL
		2 = UPDATE ALL
		4 = REFERENCES ALL
		8 = INSERT
		16 = DELETE
		32 = EXECUTE (procedures only)
		4096 = SELECT ANY (at least one column)
		8192 = UPDATE ANY
		16384 = REFERENCES ANY
Reads	16	Número de lecturas al disco lógico del servidor en nombre del evento.
RoleName	38	Nombre del rol de la aplicación que está habilitado.
Server Name	26	Nombre de la instancia de SQL Server que está habilitado.
Severity	20	Nivel de severidad de una excepción.
SPID	12	Número de identificación del proceso asignado por SQL Server para el proceso asociado con el cliente.

Start Time	14	Tiempo de inicio del evento.
State	30	Equivalente a un código de estado de error.
Success	23	Valor de resultado del evento: 1: exitoso, los permisos verificados exitosamente. 2: error /falla al verificar los permisos
TargetLoginName	42	Para acciones asociadas a inicios de sesión (por ejemplo: agregar un nuevo login) el nombre del login específico.
TargetLoginSid	43	Para acciones asociadas a inicios de sesión (por ejemplo: agregar un nuevo login) el SID del login específico.
TargetUserName	39	Para acciones asociadas a un usuario de base de datos, por ejemplo: otorgar permisos a un usuario.
TextData	1	Texto descriptivo del evento capturado en la traza. Si se captura una query con parámetros las variables no serán mostradas con valores de datos en la columna TextData.
Transaction ID	4	Número de identificación asignado a la transacción.
Writes	17	Número de escrituras físicas en el disco del servidor en nombre del evento.

Anexo XI: Vistas de SQL Audit de Sql Server

Vista	Descripción
Sys.dm_server_audits_status	Retorna una fila por cada auditoria de servidor indicando el estado actual de la auditoria.
Sys.dm_audit_actions	Retorna una fila por cada acción de auditoria que puede ser reportada en el log de auditoria y todo action group que puede ser configurado como parte de una auditoria
Sys.dm_audits_class_type_map	Retorna una tabla que mapea los tipos de clases a descripciones de clases.
Sys.server_audits	Contiene una fila por cada auditoria de SQL Server en una instancia de servidor
Sys.server_audit_specifications_details	Contiene información sobre el detalle de las especificaciones (acciones) en una auditoria a nivel de servidor en una auditoria de SQL Server
Sys.database_audit_specifications	Contiene información sobre las especificaciones de auditoria a nivel de base de datos en una auditoria de SQL Server
Sys.database_audit_specifications_details	Contiene información sobre las especificaciones (acciones) de auditoria a nivel de base de datos en una auditoria de SQL Server
Sys.server_audit_specifications	Contiene información sobre las especificaciones de auditoria a nivel de servidor en una auditoria de SQL Server

Anexo XII: Opciones de auditoria por defecto de Oracle

ALTER SYSTEM
SYSTEM AUDIT
CREATE SESSION
CREATE USER
ALTER USER
DROP USER
ROLE
CREATE ANY TABLE
ALTER ANY TABLE
DROP ANY TABLE
CREATE PUBLIC DATABASE LINK
GRANT ANY ROLE
ALTER DATABASE
CREATE ANY PROCEDURE
ALTER ANY PROCEDURE
DROP ANY PROCEDURE
ALTER PROFILE
DROP PROFILE
GRANT ANY PRIVILEGE
CREATE ANY LIBRARY
EXEMPT ACCESS POLICY
GRANT ANY OBJECT PRIVILEGE
CREATE ANY JOB
CREATE EXTERNAL JOB

Anexo XIII: Comandos a auditar de Oracle

Nombre corte de la sentencia SQL	Sentencia SQL y operación auditada
ALTER SYSTEM	ALTER SYSTEM
CLUSTER	CREATE CLUSTER ALTER CLUSTER DROP CLUSTER TRUNCATE CLUSTER
CONTEXT	CREATE CONTEXT DROP CONTEXT
DATABASE LINK	CREATE DATABASE LINK ALTER DATABASE LINK DROP DATABASE LINK
DIMENSION	CREATE DIMENSION ALTER DIMENSION DROP DIMENSION
DIRECTORY	CREATE DIRECTORY DROP DIRECTORY
INDEX	CREATE INDEX ALTER INDEX ANALYZE INDEX DROP INDEX
MATERIALIZED VIEW	CREATE MATERIALIZED VIEW ALTER MATERIALIZED VIEW DROP MATERIALIZED VIEW
NOT EXISTS	Todas las sentencias SQL que fallan porque no existe el objeto.
OUTLINE	CREATE OUTLINE ALTER OUTLINE DROP OUTLINE

Nombre corte de la sentencia SQL	Sentencia SQL y operación auditada
PROCEDURE	CREATE FUNCTION CREATE LIBRARY CREATE PACKAGE CREATE PACKAGE BODY CREATE PROCEDURE DROP FUNCTION DROP LIBRARY DROP PACKAGE DROP PROCEDURE
PROFILE	CREATE PROFILE ALTER PROFILE DROP PROFILE
PUBLIC DATABASE LINK	CREATE PUBLIC DATABASE LINK ALTER PUBLIC DATABASE LINK DROP PUBLIC DATABASE LINK
PUBLIC SYNONYM	CREATE PUBLIC SYNONYM DROP PUBLIC SYNONYM
ROLE	CREATE ROLE ALTER ROLE DROP ROLE SET ROLE
ROLLBACK SEGMENT	CREATE ROLLBACK SEGMENT ALTER ROLLBACK SEGMENT DROP ROLLBACK SEGMENT
SEQUENCE	CREATE SEQUENCE DROP SEQUENCE
SESSION	Inicios de sesión
SYNONYM	CREATE SYNONYM DROP SYNONYM

Nombre corte de la sentencia SQL	Sentencia SQL y operación auditada
SYSTEM AUDIT	AUDIT sql_statements NOAUDIT sql_statements
SYSTEM GRANT	GRANT system_privileges_and_roles REVOKE system_privileges_and_roles
TABLE	CREATE TABLE DROP TABLE TRUNCATE TABLE
TABLESPACE	CREATE TABLESPACE ALTER TABLESPACE DROP TABLESPACE
TRIGGER	CREATE TRIGGER ALTER TRIGGER DROP TRIGGER ALTER TABLE
TYPE	CREATE TYPE CREATE TYPE BODY ALTER TYPE DROP TYPE DROP TYPE BODY
USER	CREATE USER ALTER USER DROP USER
VIEW	CREATE VIEW DROP VIEW

Anexo XIV: Tablas con registros de eventos de Oracle

DBA_AUDIT_TRAIL

Column	Datatype	Description
OS_USERNAME	VARCHAR2(255)	Nombre del usuario que inicia sesión en el sistema operativo y cuyas acciones serán auditadas
USERNAME	VARCHAR2(30)	Nombre del usuario cuyas acciones serán auditadas.
USERHOST	VARCHAR2(128)	Nombre de la máquina o host del cliente
TERMINAL	VARCHAR2(255)	Identificador de la terminal del usuario
TIMESTAMP	DATE	Fecha y hora de la creación en el registro de eventos. Tiene en cuenta el tiempo de la sesión local en la base de datos.
OWNER	VARCHAR2(30)	Creador del objeto afectado en la acción
OBJ_NAME	VARCHAR2(128)	Nombre del objeto afectado por la acción
ACTION	NUMBER	Código numérico del tipo de acción.
ACTION_NAME	VARCHAR2(28)	Nombre de la acción correspondiente al código numérico.
NEW_OWNER	VARCHAR2(30)	Dueño del objeto nombrado en la columna NEW_NAME
NEW_NAME	VARCHAR2(128)	Nuevo nombre del objeto o el nombre del objeto subrayado
OBJ_PRIVILEGE	VARCHAR2(16)	Privilegios otorgados o revocados por un GRANT o REVOKE
SYS_PRIVILEGE	VARCHAR2(40)	Privilegios del sistema otorgados o revocados por un GRANT o REVOKE
ADMIN_OPTI	VARCHAR2(	Indica que roles o privilegios del sistema

ON	1)	fueron otorgados con la opción ADMIN
GRANTEE	VARCHAR2(30)	Nombre de lo otorgado especificamente en una sentencia GRANT o REVOKE
AUDIT_OPTION	VARCHAR2(40)	Opción de auditoria configurada con la sentencia AUDIT
SES_ACTIONS	VARCHAR2(19)	Resumen de la sesión, 16 caracteres por cada acción. Por ejemplo: ALTER,AUDIT, COMMENT, DELETE,GRANT, INDEX, INSERT, LOCK,RENAME, SELECT, UPDATE,REFERENCES, y EXECUTE. Las posiciones 14, 15, y 16 son reservadas para uso futuro.
LOGOFF_TIME	DATE	Fecha y hora del cierre de sesión
LOGOFF_LREAD	NUMBER	Lecturas lógicas por session
LOGOFF_PREAD	NUMBER	Lecturas físicas por sesión
LOGOFF_LWRITE	NUMBER	Escrituras físicas por sesión
LOGOFF_DLOCK	VARCHAR2(40)	Bloqueos detectados durante la sesión
COMMENT_TEXT	VARCHAR2(4000)	Comentarios adicionales sobre el registro de eventos, provee mayor información sobre la sentencia auditada.
		Indica como el usuario fue autenticado. El método puede ser uno de los siguientes:
		DATABASE - La autenticación fue hecha a través de una clave

		□ NETWORK - La autenticación fue hecha por Oracle Net Services o la opción Advanced Security
		□ PROXY - El cliente fue autenticado por otro usuario a través de un proxy.
SESSIONID	NUMBER	Número de identificación para cada sesión de Oracle
ENTRYID	NUMBER	Número de identificación para cada entrada al registro de evento de auditoria en la sesión
STATEMENTID	NUMBER	Número de identificación para cada sentencia que se ejecuta
RETURNCODE	NUMBER	Código de error de Oracle generado por la acción. Algunos valores son:
		□ 0 - Acción exitosa
		□ 2004 - violación de seguridad
PRIV_USED	VARCHAR2(40)	Privilegio de sistema usado para ejecutar la acción
CLIENT_ID	VARCHAR2(64)	Identificador del cliente en cada sesión de Oracle
ECONTEXT_ID	VARCHAR2(64)	Identificador del contexto de ejecución de la aplicación
SESSION_CPU	NUMBER	Cantidad de tiempo de CPU usado por cada sesión de Oracle
EXTENDED_TIMESTAMP	TIMESTAMP(6) WITH TIME ZONE	Tiempo de la creación de la entrada del registro de evento de auditoria
PROXY_SESSIONID	NUMBER	Número serial de la sesión de proxy, si un usuario inicio sesión a través del mecanismo de proxy
GLOBAL_UID	VARCHAR2(	Identificador global del usuario

	32)	
INSTANCE_NUMBER	NUMBER	Número de instancia especificado por el parámetro de inicialización INSTANCE_NUMBER
OS_PROCESS	VARCHAR2(16)	Identificador del proceso del sistema operativo del proceso de Oracle
TRANSACTIONID	RAW(8)	Identificador de la transacción en la cual el objeto es accedido o modificado
SCN	NUMBER	Número de cambio del sistema en la consulta
SQL_BIND	NVARCHAR2(2000)	Datos de la variable en la consulta
SQL_TEXT	NVARCHAR2(2000)	Texto de SQL en la consulta

DBA_AUDIT_STATEMENT [13]

Columna	**Tipo de dato**	**Descripción**
OS_USERNAME	VARCHAR2(255)	Nombre del usuario que inicia sesión en el sistema operativo y cuyas acciones serán auditadas
USERNAME	VARCHAR2(30)	Nombre del usuario cuyas acciones serán auditadas.
USERHOST	VARCHAR2(128)	Nombre de la máquina o host del cliente
TERMINAL	VARCHAR2(255)	Identificador de la terminal del usuario
TIMESTAMP	DATE	Fecha y hora de la creación en el registro de eventos. Tiene en cuenta el tiempo de la sesión local en la base de datos.
OWNER	VARCHAR2(30)	Creador del objeto afectado en la acción

OBJ_NAME	VARCHAR2(128)	Nombre del objeto afectado por la acción
ACTION_NAME	VARCHAR2(28)	Nombre de la acción correspondiente al código numérico.
NEW_NAME	VARCHAR2(128)	Nuevo nombre del objeto o el nombre del objeto subrayado
OBJ_PRIVILEGE	VARCHAR2(16)	Privilegios otorgados o revocados por un GRANT o REVOKE
SYS_PRIVILEGE	VARCHAR2(40)	Privilegios del sistema otorgados o revocados por un GRANT o REVOKE
ADMIN_OPTION	VARCHAR2(1)	Indica que roles o privilegios del sistema fueron otorgados con la opción ADMIN
GRANTEE	VARCHAR2(30)	Nombre de lo otorgado especificamente en una sentencia GRANT o REVOKE
AUDIT_OPTION	VARCHAR2(40)	Opción de auditoria configurada con la sentencia AUDIT
SES_ACTIONS	VARCHAR2(19)	Resumen de la sesión, 16 caracteres por cada acción. Por ejemplo: ALTER,AUDIT, COMMENT, DELETE,GRANT, INDEX, INSERT, LOCK,RENAME, SELECT,

		UPDATE,REFERENCES, y EXECUTE. Las posiciones 14, 15, y 16 son reservadas para uso futuro.
COMMENT_TEXT	VARCHAR2(4000)	Comentarios adicionales sobre el registro de eventos, provee mayor información sobre la sentencia auditada.
SESSIONID	NUMBER	Número de identificación para cada sesión de Oracle
ENTRYID	NUMBER	Número de identificación para cada entrada al registro de evento de auditoria en la sesión
STATEMENTID	NUMBER	Número de identificación para cada sentencia que se ejecuta
RETURNCODE	NUMBER	Código de error de Oracle generado por la acción. Algunos valores son: • 0 - Acción exitosa • 2004 - violación de seguridad
PRIV_USED	VARCHAR2(40)	Privilegio de sistema usado para ejecutar la acción
CLIENT_ID	VARCHAR2(64)	Identificador del cliente en cada sesión de Oracle
ECONTEXT_ID	VARCHAR2(64)	Identificador del contexto de ejecución de la aplicación
SESSION_CPU	NUMBER	Cantidad de tiempo de CPU usadp por cada

		sesión de Oracle
EXTENDED_TIMESTAMP	TIMESTAMP(6) WITH TIME ZONE	Tiempo de la creación de la entrada del registro de evento de auditoria
PROXY_SESSIONID	NUMBER	Número serial de la sesión de proxy, si un usuario inicio sesión a través del mecanismo de proxy
GLOBAL_UID	VARCHAR2(32)	Identificador global del usuario
INSTANCE_NUMBER	NUMBER	Número de instancia especificado por el parámetro de inicialización INSTANCE_NUMBER
OS_PROCESS	VARCHAR2(16)	Identificador del proceso del sistema operativo del proceso de Oracle
TRANSACTIONID	RAW(8)	Identificador de la transacción en la cual el objeto es accedido o modificado
SCN	NUMBER	Número de cambio del sistema en la consulta
SQL_BIND	NVARCHAR2(2000)	Datos de la variable en la consulta
SQL_TEXT	NVARCHAR2(2000)	Texto de SQL en la consulta

DBA_AUDIT_SESSION [14]

Columna	**Tipo de dato**	**Descripción**
OS_USERNAME	VARCHAR2(255)	Nombre del usuario que inicia sesión en el

		sistema operativo y cuyas acciones serán auditadas
USERNAME	VARCHAR2(30)	Nombre del usuario cuyas acciones serán auditadas.
USERHOST	VARCHAR2(128)	Nombre de la máquina o host del cliente
TERMINAL	VARCHAR2(255)	Identificador de la terminal del usuario
TIMESTAMP	DATE	Fecha y hora de la creación en el registro de eventos. Tiene en cuenta el tiempo de la sesión local en la base de datos.
ACTION_NAME	VARCHAR2(28)	Nombre de la acción correspondiente al código numérico.
LOGOFF_TIME	DATE	Fecha y hora que el usuario cierra sesión
LOGOFF_LREAD	NUMBER	Lecturas lógicas para la sesión
LOGOFF_PREAD	NUMBER	Lecturas físicas para la sesión
LOGOFF_LWRITE	NUMBER	Escrituras lógicas para la sesión
LOGOFF_DLOCK	VARCHAR2(40)	Bloqueos detectados durante la sesión
SESSIONID	NUMBER	Número de identificación para cada sesión de Oracle
RETURNCODE	NUMBER	Código de error de Oracle generado por la acción. Algunos valores son:

		• 0 - Acción exitosa • 2004 - violación de seguridad
CLIENT_ID	VARCHAR2(64)	Identificador del cliente en cada sesión de Oracle
SESSION_CPU	NUMBER	Cantidad de tiempo de CPU usado por cada sesión de Oracle
EXTENDED_TIMESTAMP	TIMESTAMP(6) WITH TIME ZONE	Estampa de tiempo de la creación de la entrada del registro de evento de auditoria
PROXY_SESSIONID	NUMBER	Número serial de la sesión de proxy, si un usuario inicio sesión a través del mecanismo de proxy
GLOBAL_UID	VARCHAR2(32)	Identificador global del usuario
INSTANCE_NUMBER	NUMBER	Número de instancia especificado por el parámetro de inicialización INSTANCE_NUMBER
OS_PROCESS	VARCHAR2(16)	Identificador del proceso del sistema operativo del proceso de Oracle

DBA_AUDIT_OBJECT [15]

Columna	**Tipo de dato**	**Descripción**
OS_USERNAME	VARCHAR2(255)	Nombre del usuario que inicia sesión en el sistema operativo y cuyas acciones serán auditadas

USERNAME	VARCHAR2(30)	Nombre del usuario cuyas acciones serán auditadas.
USERHOST	VARCHAR2(128)	Nombre de la máquina o host del cliente
TERMINAL	VARCHAR2(255)	Identificador de la terminal del usuario
TIMESTAMP	DATE	Fecha y hora de la creación en el registro de eventos. Tiene en cuenta el tiempo de la sesión local en la base de datos.
OWNER	VARCHAR2(30)	Creador del objeto afectado en la acción
OBJ_NAME	VARCHAR2(128)	Nombre del objeto afectado por la acción
ACTION_NAME	VARCHAR2(28)	Nombre de la acción correspondiente al código numérico.
NEW_OWNER	VARCHAR2(30)	Dueño del objeto nombrado en la columna NEW_NAME
NEW_NAME	VARCHAR2(128)	Nuevo nombre del objeto o el nombre del objeto subrayado
SES_ACTIONS	VARCHAR2(19)	Resumen de la sesión, 16 caracteres por cada acción. Por ejemplo: ALTER,AUDIT, COMMENT, DELETE,GRANT, INDEX, INSERT, LOCK,RENAME, SELECT, UPDATE,REFERENCES, y EXECUTE. Las posiciones 14, 15, y 16 son reservadas para uso futuro.

COMMENT_TEXT	VARCHAR2(4000)	Comentarios adicionales sobre el registro de eventos, provee mayor información sobre la sentencia auditada.
SESSIONID	NUMBER	Número de identificación para cada sesión de Oracle
ENTRYID	NUMBER	Número de identificación para cada entrada al registro de evento de auditoria en la sesión
STATEMENTID	NUMBER	Número de identificación para cada sentencia que se ejecuta
RETURNCODE	NUMBER	Código de error de Oracle generado por la acción. Algunos valores son: · 0 - Acción exitosa · 2004 - violación de seguridad
PRIV_USED	VARCHAR2(40)	Privilegio de sistema usado para ejecutar la acción
CLIENT_ID	VARCHAR2(64)	Identificador del cliente en cada sesión de Oracle
ECONTEXT_ID	VARCHAR2(64)	Identificador del contexto de ejecución de la aplicación
SESSION_CPU	NUMBER	Cantidad de tiempo de CPU usadp por cada sesión de Oracle
EXTENDED_TIMESTAMP	TIMESTAMP(6) WITH TIME ZONE	Tiempo de la creación de la entrada del registro de evento de auditoria
PROXY_SESSIONID	NUMBER	Número serial de la sesión de proxy, si un usuario inicio sesión a través del mecanismo de proxy
GLOBAL_UID	VARCHAR2(32)	Identificador global del usuario

INSTANCE_NUMBER	NUMBER	Número de instancia especificado por el parámetro de inicialización INSTANCE_NUMBER
OS_PROCESS	VARCHAR2(16)	Identificador del proceso del sistema operativo del proceso de Oracle
TRANSACTIONID	RAW(8)	Identificador de la transacción en la cual el objeto es accedido o modificado
SCN	NUMBER	Número de cambio del sistema en la consulta
SQL_BIND	NVARCHAR2(2000)	Datos de la variable en la consulta
SQL_TEXT	NVARCHAR2(2000)	Texto de SQL en la consulta

DBA_AUDIT_EXISTS [16]

Columna	**Tipo de dato**	**Descripción**
OS_USERNAME	VARCHAR2(255)	Nombre del usuario que inicia sesión en el sistema operativo y cuyas acciones serán auditadas
USERNAME	VARCHAR2(30)	Nombre del usuario cuyas acciones serán auditadas.
USERHOST	VARCHAR2(128)	Nombre de la máquina o host del cliente
TERMINAL	VARCHAR2(255)	Identificador de la terminal del usuario
TIMESTAMP	DATE	Fecha y hora de la creación en el registro de eventos. Tiene en cuenta el tiempo de la sesión local en la base de datos.
OWNER	VARCHAR2(30)	Creador del objeto afectado en la acción

OBJ_NAME	VARCHAR2(128)	Nombre del objeto afectado por la acción
ACTION_NAME	VARCHAR2(28)	Nombre de la acción correspondiente al código numérico.
NEW_OWNER	VARCHAR2(30)	Dueño del objeto nombrado en la columna NEW_NAME
NEW_NAME	VARCHAR2(128)	Nuevo nombre del objeto o el nombre del objeto subrayado
OBJ_PRIVILEGE	VARCHAR2(16)	Privilegios otorgados o revocados por un GRANT o REVOKE
SYS_PRIVILEGE	VARCHAR2(40)	Privilegios del sistema otorgados o revocados por un GRANT o REVOKE
GRANTEE	VARCHAR2(30)	Nombre de lo otorgado especificamente en una sentencia GRANT o REVOKE
SESSIONID	NUMBER	Número de identificación para cada sesión de Oracle
ENTRYID	NUMBER	Número de identificación para cada entrada al registro de evento de auditoria en la sesión
STATEMENTID	NUMBER	Número de identificación para cada sentencia que se ejecuta
RETURNCODE	NUMBER	Código de error de Oracle generado por la acción. Algunos valores son: · 0 - Acción exitosa · 2004 - violación de seguridad
CLIENT_ID	VARCHAR2(64)	Identificador del cliente en cada sesión de Oracle

ECONTEXT_ID	VARCHAR2(64)	Identificador del contexto de ejecución de la aplicación
SESSION_CPU	NUMBER	Cantidad de tiempo de CPU usado por cada sesión de Oracle
EXTENDED_TIMESTAMP	TIMESTAMP(6) WITH TIME ZONE	Estampa de tiempo de la creación de la entrada del registro de evento de auditoria
PROXY_SESSIONID	NUMBER	Número serial de la sesión de proxy, si un usuario inicio sesión a través del mecanismo de proxy
GLOBAL_UID	VARCHAR2(32)	Identificador global del usuario
INSTANCE_NUMBER	NUMBER	Número de instancia especificado por el parámetro de inicialización INSTANCE_NUMBER
OS_PROCESS	VARCHAR2(16)	Identificador del proceso del sistema operativo del proceso de Oracle
TRANSACTIONID	RAW(8)	Identificador de la transacción en la cual el objeto es accedido o modificado
SCN	NUMBER	Número de cambio del sistema en la consulta
SQL_BIND	NVARCHAR2(2000)	Datos de la variable en la consulta
SQL_TEXT	NVARCHAR2(2000)	Texto de SQL en la consulta
OBJ_EDITION_NAME	VARCHAR2(30)	Reservado para uso futuro

V$XML_AUDIT_TRAIL [17]

Incluye los archivos en formato xml

Columna	Tipo de dato	Descripción
AUDIT_TYPE	NUMBER	Tipo de auditoria 1 = Standard XML Audit 2 = Fine Grained XML Audit 4 = SYS XML Audit 8 = Mandatory XML Audit
SESSION_ID	NUMBER	Número de identificación para cada sesión de Oracle
PROXY_SESSIONID	NUMBER	Número serial de la sesión de proxy, si un usuario inicio sesión a través del mecanismo de proxy
STATEMENTID	NUMBER	Número de identificación para cada sentencia que se ejecuta
ENTRYID	NUMBER	Número de identificación para cada entrada al registro de evento de auditoria en la sesión
EXTENDED_TIMESTAMP	TIMESTAMP(6) WITH TIME ZONE	Tiempo de la creación de la entrada del registro de evento de auditoria
GLOBAL_UID	VARCHAR2(32)	Identificador global del usuario
DB_USER	VARCHAR2(30)	Usuario de la base de datos
CLIENTIDENTIFIER	VARCHAR2(64)	Identificador del cliente en la sesión de Oracle
EXT_NAME	VARCHAR2(1024)	Nombre del usuario externo
OS_USER	VARCHAR2(30)	Nombre del usuario que inicia sesión en el sistema operativo
OS_HOST	VARCHAR2(128)	Nombre de la máquina o host del cliente
OS_PROCESS	VARCHAR2(16)	Identificador del proceso del

		sistema operativo del proceso de Oracle
TERMINAL	VARCHAR2(30)	Identificador de la terminal del usuario
INSTANCE_NUMBER	NUMBER	Número de instancia especificado por el parámetro de inicialización INSTANCE_NUMBER
OBJECT_SCHEMA	VARCHAR2(30)	Dueño del objeto
OBJECT_NAME	VARCHAR2(30)	Nombre del objeto
POLICY_NAME	VARCHAR2(30)	Nombre de la política de auditoria fine-grained
NEW_OWNER	VARCHAR2(30)	Dueño del objeto nombrado en la columna NEW_NAME
NEW_NAME	VARCHAR2(30)	Nuevo nombre del objeto o el nombre del objeto subrayado
ACTION	NUMBER	Nombre de la acción correspondiente al código numérico.
STATEMENT_TYPE	NUMBER	Descripción de la acción
TRANSACTIONID	RAW(8)	Identificador de la transacción en la cual el objeto es accedido o modificado
RETURNCODE	NUMBER	Código de error de Oracle generado por la acción. Cero significa que la acción fue exitosa
SCN	NUMBER	Número de cambio del sistema de la consulta
COMMENT_TEXT	VARCHAR2(4000)	Comentarios adicionales sobre el registro de eventos, provee mayor información sobre la sentencia auditada
AUTH_PRIVILEGES	VARCHAR2(16)	Privilegios otorgados y revocados con sentencias GRANT y

		REVOKE
GRANTEE	VARCHAR2(30)	Usuario al que se otorgo el privilegio
PRIV_USED	NUMBER	Código numérico del privilegio si se utilizó en una acción
SES_ACTIONS	VARCHAR2(16)	Resumen de la sesión, 12 caracteres por cada acción
OS_PRIVILEGE	VARCHAR2(7)	Privilegio del sistema operativo (Sysdba o SysOper). Si no se usa el privilegio se completa con NONE
ECONTEXT_ID	VARCHAR2(64)	Identificador del contexto de ejecución de la aplicación
SQL_BIND	VARCHAR2(4000)	Datos de la variable en la consulta
SQL_TEXT	VARCHAR2(4000)	Texto de SQL en la consulta
OBJ_EDITION_NAME	VARCHAR2(30)	Nombre de la edición contenida en el objeto auditado
DBID	NUMBER	Identificador de la base de datos auditada

DBA_FGA_AUDIT_TRAIL

Columna	**Tipo de dato**	**Descripción**
SESSION_ID	NUMBER	Número de identificación de la consulta
TIMESTAMP	DATE	Fecha y hora de la consulta en el horario de la base de datos local
DB_USER	VARCHAR2(30)	Usuario de la base de datos que ejecutó la consulta
OS_USER	VARCHAR2(255)	Usuario del sistema operativo que ejecutó la consulta

USERHOST	VARCHAR2(128)	Nombre de la máquina /host del cliente
CLIENT_ID	VARCHAR2(64)	Identificador del cliente en cada sesión de Oracle
ECONTEXT_ID	VARCHAR2(64)	Identificador del contexto de ejecución de la aplicación
EXT_NAME	VARCHAR2(4000)	Nombre externo
OBJECT_SCHEMA	VARCHAR2(30)	Dueño de la tabla o vista
OBJECT_NAME	VARCHAR2(128)	Nombre de la tabla o vista
POLICY_NAME	VARCHAR2(30)	Nombre de la política Fine-Grained Auditing
SCN	NUMBER	Número de cambio del sistema (SCN) de la consulta
SQL_TEXT	NVARCHAR2(2000)	Texto de SQL de la consulta
SQL_BIND	NVARCHAR2(2000)	Datos de la variable en la consulta
COMMENT$TEXT	VARCHAR2(4000)	Comentarios
STATEMENT_TYPE	VARCHAR2(7)	Tipos de sentencias de la consulta: SELECT INSERT UPDATE DELETE
EXTENDED_TIMESTAMP	TIMESTAMP(6) WITH TIME ZONE	Tiempo en la consulta en UTC (Coordinated Universal Time)

PROXY_SESSIONID	NUMBER	Número serial de la sesión proxy, si un usuario se ha registrado a través del mecanismo de proxy
GLOBAL_UID	VARCHAR2(32)	Identificador del usuario global, si el usuario se ha registrado como un usuario empresarial
INSTANCE_NUMBER	NUMBER	Número de instancia se especifica en el parámetro INSTANCE_NUMBER
OS_PROCESS	VARCHAR2(16)	Identificador del proceso de sistema operativo del proceso Oracle
TRANSACTIONID	RAW(8)	Identificador de la transacción por la cual el objeto se accedió o modificó
STATEMENTID	NUMBER	Número de identificación por cada sentencia que se ejecuta (una sentencia puede causar muchas acciones)
ENTRYID	NUMBER	Número de identificación por cada entrada en el registro de eventos

UNIFIED_AUDIT_TRAIL

Columna	**Tipo de dato**	**Descripción**
AUDIT_TYPE	VARCHAR2(64)	Tipo de auditoria:
		· Standard
		· FineGrainedAudit
		· XS
		· Database Vault
		· Label Security
		· RMAN_AUDIT
		· Datapump
		· Direct path API
SESSIONID	NUMBER	Identificador de la sesión de auditoria

PROXY_SESSIONID	NUMBER	Identificador de la sesión de auditoria de la sesión proxy
OS_USERNAME	VARCHAR2(30)	Nombre del usuario de sistema operativo para la sesión de base de datos
USERHOST	VARCHAR2(128)	Nombre del host para la cual la sesión fue generada
TERMINAL	VARCHAR2(30)	Sistema operativo de la terminal desde la cual el usuario tiene sesión
INSTANCE_ID	NUMBER	Número de instancia especificada en el parámetro file del archivo init.ora
DBID	NUMBER	Identificador de la base de datos de la base de datos auditada
AUTHENTICATION_TYPE	VARCHAR2(1024)	Tipo de autenticación de la sesión de usuario
DBUSERNAME	VARCHAR2(30)	Nombre del usuario de la base de datos cuyas acciones fueron auditadas
DBPROXY_USERNAME	VARCHAR2(30)	Nombre del usuario proxy, en caso de autenticación proxy
EXTERNAL_USERID	VARCHAR2(1024)	Nombre del usuario externo, en caso de red o autenticación externa
GLOBAL_USERID	VARCHAR2(32)	Identificador global del usuario, para un usuario registrado como usuario empresarial
CLIENT_PROGRAM_NAME	VARCHAR2(48)	Nombre del programa usado para la sesión de base de datos
DBLINK_INFO	VARCHAR2(4000)	Valor de SYS_CONTEXT('USERENV','DBLINK_INFO'). Valida si la conexión fue un enlace a la base de datos
XS_USER_NAME	VARCHAR2(128)	Nombre del usuario Real Application Security
XS_SESSIONID	RAW(33)	Identificador de la sesión Real

		Application Security
ENTRY_ID	NUMBER	Número de identificación para cada entrada del registro de evento en la sesión
STATEMENT_ID	NUMBER	Número de identificación de cada sentencia que se ejecuta
EVENT_TIMESTAMP	TIMESTAMP(6) WITH LOCAL TIME ZONE	Tiempo de creación de la entrada del registro de auditoria en UTC
ACTION_NAME	VARCHAR2(64)	Nombre de la acción ejecutada por el usuario. El nombre podría ser leido en conjunción con AUDIT_TYPE para entender la acción real
RETURN_CODE	NUMBER	Código de error de Oracle generado por la acción. Cero representa que la acción fue exitosa
OS_PROCESS	VARCHAR2(16)	Identificador del proceso del sistema operativo del proceso de la base de datos Oracle
TRANSACTION_ID	RAW(8)	Identificador de la transacción en la cual el objeto fue modificado
SCN	NUMBER	Número de cambio del sistema (SCN) de la consulta
EXECUTION_ID	VARCHAR2(64)	Identificador del contexto por cada acción
OBJECT_SCHEMA	VARCHAR2(30)	Nombre del esquema del objeto afectado por la acción
OBJECT_NAME	VARCHAR2(128)	Nombre del objeto afectado por la acción
SQL_TEXT	CLOB	SQL asociado con el evento
SQL_BINDS	CLOB	Lista de variables, si alguna esta asociada con SQL_TEXT

APPLICATION_CONTEXTS	VARCHAR2(4000)	Lista separadas por comas sobre el detalle del contexto de la aplicación. Por ejemplo: Application Context Namespace, Attribute, Value information en formato (APPCTX_NSPACE,APPCTX_ATTRIBUTE=<value>)
CLIENT_IDENTIFIER	VARCHAR2(64)	Identificador del cliente en cada sesión de Oracle
NEW_SCHEMA	VARCHAR2(30)	El esquema del objeto nombrado en la columna NEW_NAME
NEW_NAME	VARCHAR2(128)	Nombre del objeto después de RENAME o nombre del objeto subrayado (por ejemplo: CREATE INDEX owner.obj_name ON new_owner.new_name)
OBJECT_EDITION	VARCHAR2(30)	Nombre de la edición contenida en el objeto auditado
SYSTEM_PRIVILEGE_USED	VARCHAR2(1024)	Lista separada por comas de los privilegios de sistema usados para la ejecución de la acción
SYSTEM_PRIVILEGE	VARCHAR2(40)	Privilegio de sistema otorgado/revocado por la sentencia GRANT/REVOKE
AUDIT_OPTION	VARCHAR2(40)	Comando SQL AUDIT/NOAUDIT SQL
OBJECT_PRIVILEGES	VARCHAR2(19)	Privilegios de objeto otorgado/revocado por la sentencia GRANT/REVOKE
ROLE	VARCHAR2(30)	Roles otorgados o revocados o configurador por el comando GRANT/REVOKE/SET ROLE
TARGET_USER	VARCHAR2(30)	Usuario que ejecutó la sentencia GRANT/REVOKE/AUDIT/NOAUDIT

EXCLUDED_USER	VARCHAR2(30)	Usuario que fue excluído cuando se ejecutó AUDIT/NOAUDIT
EXCLUDED_SCHEMA	VARCHAR2(30)	Muestra el esquema de objetos excluidos
EXCLUDED_OBJECT	VARCHAR2(128)	Muestra los objetos excluidos desde la acción
ADDITIONAL_INFO	VARCHAR2(4000)	Texto comentado sobre la entrada del registro de eventos de auditoria
UNIFIED_AUDIT_POLICIES	VARCHAR2(4000)	Listado de las políticas de auditoria que causan los registros de auditoria actuales. Si mas de una politica fue configurada, la lista de políticas que causaron el evento serán registradas en el registro de auditoria separadas por comas
FGA_POLICY_NAME	VARCHAR2(30)	El nombre de la política Fine-grained auditing (FGA)
XS_INACTIVITY_TIMEOUT	NUMBER	Tiempo límite de inactividad de la sesión Real Application Security
XS_ENTITY_TYPE	VARCHAR2(32)	Tipo de la entidad Real Application Security. Valores posibles USER, ROLE, ROLESET, SECURITY CLASS, ACL,DATASECURITY y NSTEMPLATE.
XS_TARGET_PRINCIPAL_NAME	VARCHAR2(30)	Nombre de las operaciones en Real Application Security. Operaciones posibles set verifier, set password, add proxy, remove proxy, switch user, assign user, create session, y grant roles.
XS_PROXY_USER_NAME	VARCHAR2(30)	Nombre del proxy user Real Application Security

XS_DATASEC_POLICY_NAME	VARCHAR2(30)	Nombre de la política de seguridad habilitada o inhabilitada de Real Application Security
XS_SCHEMA_NAME	VARCHAR2(30)	Nombre del esquema habilitado, política de seguridad de datos inhabilitada y operación global de retorno
XS_CALLBACK_EVENT_TYPE	VARCHAR2(32)	Tipo de evento callback Real Application Security
XS_PACKAGE_NAME	VARCHAR2(30)	Nombre de paquete global de callback de Real Application Security
XS_PROCEDURE_NAME	VARCHAR2(30)	Nombre de procedimiento global de callback de Real Application Security
XS_ENABLED_ROLE	VARCHAR2(30)	El rol que esta habilitado
XS_COOKIE	VARCHAR2(1024)	Cookie de sesión Real Application Security
XS_NS_NAME	VARCHAR2(30)	Nombre de la sesión namespace de Real Application Security
XS_NS_ATTRIBUTE	VARCHAR2(4000)	Nombre del atributo del namespace de Real Application Security
XS_NS_ATTRIBUTE_OLD_VAL	VARCHAR2(4000)	El valor antiguo del atributo namespace sesion del Real Application Security
XS_NS_ATTRIBUTE_NEW_VAL	VARCHAR2(4000)	El valor nuevo del atributo namespace sesion del Real Application Security
DV_ACTION_CODE	NUMBER	Código del número de una acción para Database Vault
DV_ACTION_NAME	VARCHAR2(30)	Nombre de la acción correspondiente al código que aparece en la columna DV_ACTION_CODE
DV_EXTENDED_ACTION_COD	NUMBER	Código númerico de la acción para la administración de Database Vault

E		
DV_GRANTEE	VARCHAR2(30)	Nombre del usuario que fue modificado en Database Vault
DV_RETURN_CODE	NUMBER	Código de error en Database Vault
DV_ACTION_OBJECT_NAME	VARCHAR2(128)	El nombre único del objeto modificado de Database Vault
DV_RULE_SET_NAME	VARCHAR2(90)	Nombre único de la regla que fue ejecutada y causo que se dispare un evento de auditoria
DV_COMMENT	VARCHAR2(4000)	Comentario del texto de la entrada del evento de auditoria. Brinda mayor información sobre la sentencia auditada
DV_FACTOR_CONTEXT	VARCHAR2(4000)	Un documento XML que contien todos los factores identificadores para la sesión corriente
DV_OBJECT_STATUS	VARCHAR2(1)	Indica que un objeto particular de Database Vault se habilita o inhabilita. Los valores posibles son: Y - Objeto habilitado N - Objecto inhabilitado
OLS_POLICY_NAME	VARCHAR2(30)	Nombre de la política de Oracle Label Security (OLS) por la cual el registro de auditoria se genera
OLS_GRANTEE	VARCHAR2(30)	Nombre del usuario cuya autorización OLS fue modificada
OLS_MAX_READ_LABEL	VARCHAR2(4000)	Máximo nivel de lectura asignado al usuario
OLS_MAX_WRITE_LABEL	VARCHAR2(4000)	Máximo nivel de escritura asignado al usuario
OLS_MIN_WRITE_LABEL	VARCHAR2(4000)	Mínimo nivel de escritura asignado al usuario

OLS_PRIVILEGES_GRANTED	VARCHAR2(30)	Privilegios OLS asignados para el usuario o procedimiento almacenado confiado
OLS_PROGRAM_UNIT_NAME	VARCHAR2(30)	Nombre del procedimiento almacenado de confianza cuya autorización fue modificada o fue ejecutada
OLS_PRIVILEGES_USED	VARCHAR2(128)	Privilegios OLS usados por un evento
OLS_STRING_LABEL	VARCHAR2(4000)	Cadenas de caracteres que representa el nivel OLS
OLS_LABEL_COMPONENT_TYPE	VARCHAR2(12)	Tipo del nivel del componente OLS
OLS_LABEL_COMPONENT_NAME	VARCHAR2(30)	Nombre del nivel del componente OLS
OLS_PARENT_GROUP_NAME	VARCHAR2(30)	Nombre del padre del grupo OLS
OLS_OLD_VALUE	VARCHAR2(4000)	Valor anterior para eventos OLS ALTER
OLS_NEW_VALUE	VARCHAR2(4000)	Nuevo valor para eventos OLS ALTER
RMAN_SESSION_RECID	NUMBER	Identificador de sesión RMAN
RMAN_SESSION_STAMP	NUMBER	Tiempo de la sesión
RMAN_OPERATION	VARCHAR2(20)	La operación RMAN ejecutada por el job.

RMAN_OBJECT_TYPE	VARCHAR2(20)	Tipo de objetos involucrados para el backup o recuperación o comandos de cambio/eliminación/crosscheck. Los valores posibles son: DB FULL RECVR AREA DB INCR DATAFILE FULL DATAFILE INCR ARCHIVELOG CONTROLFILE SPFILE
RMAN_DEVICE_TYPE	VARCHAR2(5)	Dispositivo involucrador en el RMAN job.
DP_TEXT_PARAMETERS1	VARCHAR2(512)	Parámetros durante una operación Data Pump que tengan un valor de texto. Los valores que puede contener son: ACCESS METHODS DATA OPTIONS DUMPER DIRECTORY JOB_TYPE JOB VERSION MASTER TABLE METADATA_JOB_MODE PARTITION OPTIONS REMOTE LINK TABLE EXISTS
DP_BOOLEAN_PARAMETERS1	VARCHAR2(512)	Parámetro durante una operación Data Pump que tenga un valor booleano

DIRECT_PATH_ NUM_COLUMN S_LOADED	NUMBER	Muestra el número de columnas que fueron levantadas usando el método SQL*Loader

Anexo XV: Opciones configuradas para los distintos sistemas de gestión de base de datos relacional

Oracle 11 g r2

alter system set AUDIT_SYS_OPERATIONS=TRUE SCOPE=SPFILE

Audit table by access;
Audit drop any table by access;
Audit create any procedure by access;
Audit drop any procedure by access;
Audit alter any procedure by access;
Audit create external job by access;
Audit create any job by access;
Audit create any library by access;
Audit alter database by access;
Audit alter system by access;
Audit directory by access;
Audit database link by access;
Audit not exists by access;
Audit create public synonym by access;
Audit drop public synonym by access;
Audit synonym by access;
Audit tablespace by access;
Audit view by access;
Audit trigger by access;
Audit audit system by access;
Audit create public database link by access;
Audit drop public database link by access;
Audit exempt access policy by access;
Audit alter user by access;
Audit create user by access;
Audit role by access;
Audit create session by access;
Audit drop user by access;

```
Audit grant any privilege by access;
Audit grant any object privilege by access;
Audit grant any role by access;
Audit alter profile by access;
Audit drop profile by access;
Audit create profile by access;
Audit system grant by access;
```

SQL Server 2012

```
Create procedure traza_si
as
set nocount on

declare @TraceIdOut int
declare @On BIT
declare @On_status int
declare @TraceFile nvarchar(254)
declare @MaxFileSize bigint
-- Id de la traza:
SET @TraceIdOut=1
-- Status del evento:
SET @On=1
-- Status de la traza:
SET @On_status=1
-- Maximo tamaño de archivo:
SET @MaxFileSize=50
-- Define 'path\archivo_fecha_hora' formato(aaaammdd_hhmmss):
select @TraceFile='F:\sql2000\AUDIT\trace'
+
'_'
+
convert(char(8),getdate(),112)
+
'_'
+
rtrim(convert(char(2),replicate('0',2-
len(rtrim(convert(char(2),datepart(hour,getdate()))))))
+
rtrim(convert(char(2),datepart(hour,getdate())))
+
rtrim(convert(char(2),replicate('0',2-
len(rtrim(convert(char(2),datepart(minute,getdate()))))))
+
rtrim(convert(char(2),datepart(minute,getdate())))
+
rtrim(convert(char(2),replicate('0',2-
len(rtrim(convert(char(2),datepart(second,getdate()))))))
+
rtrim(convert(char(2),datepart(second,getdate())))

begin
-- Primero, genera la traza:
```

```
exec sp_trace_create @TraceIdOut OUTPUT, 2, @TraceFile, @MaxFileSize
-- Segundo, setea los eventos:


exec sp_trace_setevent @TraceIdOut, 14, 6, @On
exec sp_trace_setevent @TraceIdOut, 14, 7, @On
exec sp_trace_setevent @TraceIdOut, 14, 8, @On
exec sp_trace_setevent @TraceIdOut, 14, 9, @On
exec sp_trace_setevent @TraceIdOut, 14, 10, @On
exec sp_trace_setevent @TraceIdOut, 14, 11, @On
exec sp_trace_setevent @TraceIdOut, 14, 14, @On
exec sp_trace_setevent @TraceIdOut, 14, 23, @On
exec sp_trace_setevent @TraceIdOut, 14, 27, @On
exec sp_trace_setevent @TraceIdOut, 14, 41, @On
exec sp_trace_setevent @TraceIdOut, 15, 6, @On
exec sp_trace_setevent @TraceIdOut, 15, 7, @On
exec sp_trace_setevent @TraceIdOut, 15, 8, @On
exec sp_trace_setevent @TraceIdOut, 15, 9, @On
exec sp_trace_setevent @TraceIdOut, 15, 10, @On
exec sp_trace_setevent @TraceIdOut, 15, 11, @On
exec sp_trace_setevent @TraceIdOut, 15, 13, @On
exec sp_trace_setevent @TraceIdOut, 15, 14, @On
exec sp_trace_setevent @TraceIdOut, 15, 15, @On
exec sp_trace_setevent @TraceIdOut, 15, 17, @On
exec sp_trace_setevent @TraceIdOut, 15, 18, @On
exec sp_trace_setevent @TraceIdOut, 15, 23, @On
exec sp_trace_setevent @TraceIdOut, 15, 27, @On
exec sp_trace_setevent @TraceIdOut, 15, 41, @On
exec sp_trace_setevent @TraceIdOut, 18, 6, @On
exec sp_trace_setevent @TraceIdOut, 18, 7, @On
exec sp_trace_setevent @TraceIdOut, 18, 8, @On
exec sp_trace_setevent @TraceIdOut, 18, 9, @On
exec sp_trace_setevent @TraceIdOut, 18, 10, @On
exec sp_trace_setevent @TraceIdOut, 18, 11, @On
exec sp_trace_setevent @TraceIdOut, 18, 14, @On
exec sp_trace_setevent @TraceIdOut, 18, 23, @On
exec sp_trace_setevent @TraceIdOut, 18, 27, @On
exec sp_trace_setevent @TraceIdOut, 18, 41, @On
exec sp_trace_setevent @TraceIdOut, 20, 1, @On
exec sp_trace_setevent @TraceIdOut, 20, 6, @On
exec sp_trace_setevent @TraceIdOut, 20, 7, @On
exec sp_trace_setevent @TraceIdOut, 20, 8, @On
exec sp_trace_setevent @TraceIdOut, 20, 9, @On
exec sp_trace_setevent @TraceIdOut, 20, 10, @On
exec sp_trace_setevent @TraceIdOut, 20, 11, @On
exec sp_trace_setevent @TraceIdOut, 20, 13, @On
exec sp_trace_setevent @TraceIdOut, 20, 14, @On
exec sp_trace_setevent @TraceIdOut, 20, 27, @On
exec sp_trace_setevent @TraceIdOut, 102, 1, @On
exec sp_trace_setevent @TraceIdOut, 102, 6, @On
```

```
exec sp_trace_setevent @TraceIdOut, 102, 7, @On
exec sp_trace_setevent @TraceIdOut, 102, 8, @On
exec sp_trace_setevent @TraceIdOut, 102, 9, @On
exec sp_trace_setevent @TraceIdOut, 102, 10, @On
exec sp_trace_setevent @TraceIdOut, 102, 11, @On
exec sp_trace_setevent @TraceIdOut, 102, 14, @On
exec sp_trace_setevent @TraceIdOut, 102, 19, @On
exec sp_trace_setevent @TraceIdOut, 102, 21, @On
exec sp_trace_setevent @TraceIdOut, 102, 23, @On
exec sp_trace_setevent @TraceIdOut, 102, 27, @On
exec sp_trace_setevent @TraceIdOut, 102, 35, @On
exec sp_trace_setevent @TraceIdOut, 102, 39, @On
exec sp_trace_setevent @TraceIdOut, 102, 40, @On
exec sp_trace_setevent @TraceIdOut, 102, 41, @On
exec sp_trace_setevent @TraceIdOut, 103, 1, @On
exec sp_trace_setevent @TraceIdOut, 103, 6, @On
exec sp_trace_setevent @TraceIdOut, 103, 7, @On
exec sp_trace_setevent @TraceIdOut, 103, 8, @On
exec sp_trace_setevent @TraceIdOut, 103, 9, @On
exec sp_trace_setevent @TraceIdOut, 103, 10, @On
exec sp_trace_setevent @TraceIdOut, 103, 11, @On
exec sp_trace_setevent @TraceIdOut, 103, 14, @On
exec sp_trace_setevent @TraceIdOut, 103, 19, @On
exec sp_trace_setevent @TraceIdOut, 103, 21, @On
exec sp_trace_setevent @TraceIdOut, 103, 23, @On
exec sp_trace_setevent @TraceIdOut, 103, 27, @On
exec sp_trace_setevent @TraceIdOut, 103, 34, @On
exec sp_trace_setevent @TraceIdOut, 103, 35, @On
exec sp_trace_setevent @TraceIdOut, 103, 39, @On
exec sp_trace_setevent @TraceIdOut, 103, 40, @On
exec sp_trace_setevent @TraceIdOut, 103, 41, @On
exec sp_trace_setevent @TraceIdOut, 103, 44, @On
exec sp_trace_setevent @TraceIdOut, 104, 6, @On
exec sp_trace_setevent @TraceIdOut, 104, 7, @On
exec sp_trace_setevent @TraceIdOut, 104, 8, @On
exec sp_trace_setevent @TraceIdOut, 104, 9, @On
exec sp_trace_setevent @TraceIdOut, 104, 10, @On
exec sp_trace_setevent @TraceIdOut, 104, 11, @On
exec sp_trace_setevent @TraceIdOut, 104, 14, @On
exec sp_trace_setevent @TraceIdOut, 104, 21, @On
exec sp_trace_setevent @TraceIdOut, 104, 23, @On
exec sp_trace_setevent @TraceIdOut, 104, 27, @On
exec sp_trace_setevent @TraceIdOut, 104, 41, @On
exec sp_trace_setevent @TraceIdOut, 104, 42, @On
exec sp_trace_setevent @TraceIdOut, 104, 43, @On
exec sp_trace_setevent @TraceIdOut, 105, 6, @On
exec sp_trace_setevent @TraceIdOut, 105, 7, @On
exec sp_trace_setevent @TraceIdOut, 105, 8, @On
exec sp_trace_setevent @TraceIdOut, 105, 9, @On
exec sp_trace_setevent @TraceIdOut, 105, 10, @On
```

```
exec sp_trace_setevent @TraceIdOut, 105, 11, @On
exec sp_trace_setevent @TraceIdOut, 105, 14, @On
exec sp_trace_setevent @TraceIdOut, 105, 21, @On
exec sp_trace_setevent @TraceIdOut, 105, 23, @On
exec sp_trace_setevent @TraceIdOut, 105, 27, @On
exec sp_trace_setevent @TraceIdOut, 105, 41, @On
exec sp_trace_setevent @TraceIdOut, 105, 42, @On
exec sp_trace_setevent @TraceIdOut, 105, 43, @On
exec sp_trace_setevent @TraceIdOut, 106, 6, @On
exec sp_trace_setevent @TraceIdOut, 106, 7, @On
exec sp_trace_setevent @TraceIdOut, 106, 8, @On
exec sp_trace_setevent @TraceIdOut, 106, 9, @On
exec sp_trace_setevent @TraceIdOut, 106, 10, @On
exec sp_trace_setevent @TraceIdOut, 106, 11, @On
exec sp_trace_setevent @TraceIdOut, 106, 14, @On
exec sp_trace_setevent @TraceIdOut, 106, 21, @On
exec sp_trace_setevent @TraceIdOut, 106, 23, @On
exec sp_trace_setevent @TraceIdOut, 106, 27, @On
exec sp_trace_setevent @TraceIdOut, 106, 41, @On
exec sp_trace_setevent @TraceIdOut, 106, 42, @On
exec sp_trace_setevent @TraceIdOut, 106, 43, @On
exec sp_trace_setevent @TraceIdOut, 107, 6, @On
exec sp_trace_setevent @TraceIdOut, 107, 7, @On
exec sp_trace_setevent @TraceIdOut, 107, 8, @On
exec sp_trace_setevent @TraceIdOut, 107, 9, @On
exec sp_trace_setevent @TraceIdOut, 107, 10, @On
exec sp_trace_setevent @TraceIdOut, 107, 11, @On
exec sp_trace_setevent @TraceIdOut, 107, 14, @On
exec sp_trace_setevent @TraceIdOut, 107, 21, @On
exec sp_trace_setevent @TraceIdOut, 107, 23, @On
exec sp_trace_setevent @TraceIdOut, 107, 27, @On
exec sp_trace_setevent @TraceIdOut, 107, 41, @On
exec sp_trace_setevent @TraceIdOut, 107, 42, @On
exec sp_trace_setevent @TraceIdOut, 107, 43, @On
exec sp_trace_setevent @TraceIdOut, 108, 6, @On
exec sp_trace_setevent @TraceIdOut, 108, 7, @On
exec sp_trace_setevent @TraceIdOut, 108, 8, @On
exec sp_trace_setevent @TraceIdOut, 108, 9, @On
exec sp_trace_setevent @TraceIdOut, 108, 10, @On
exec sp_trace_setevent @TraceIdOut, 108, 11, @On
exec sp_trace_setevent @TraceIdOut, 108, 14, @On
exec sp_trace_setevent @TraceIdOut, 108, 21, @On
exec sp_trace_setevent @TraceIdOut, 108, 23, @On
exec sp_trace_setevent @TraceIdOut, 108, 27, @On
exec sp_trace_setevent @TraceIdOut, 108, 38, @On
exec sp_trace_setevent @TraceIdOut, 108, 40, @On
exec sp_trace_setevent @TraceIdOut, 108, 41, @On
exec sp_trace_setevent @TraceIdOut, 108, 42, @On
exec sp_trace_setevent @TraceIdOut, 108, 43, @On
exec sp_trace_setevent @TraceIdOut, 109, 6, @On
```

```
exec sp_trace_setevent @TraceIdOut, 109, 7, @On
exec sp_trace_setevent @TraceIdOut, 109, 8, @On
exec sp_trace_setevent @TraceIdOut, 109, 9, @On
exec sp_trace_setevent @TraceIdOut, 109, 10, @On
exec sp_trace_setevent @TraceIdOut, 109, 11, @On
exec sp_trace_setevent @TraceIdOut, 109, 14, @On
exec sp_trace_setevent @TraceIdOut, 109, 21, @On
exec sp_trace_setevent @TraceIdOut, 109, 23, @On
exec sp_trace_setevent @TraceIdOut, 109, 27, @On
exec sp_trace_setevent @TraceIdOut, 109, 35, @On
exec sp_trace_setevent @TraceIdOut, 109, 38, @On
exec sp_trace_setevent @TraceIdOut, 109, 39, @On
exec sp_trace_setevent @TraceIdOut, 109, 40, @On
exec sp_trace_setevent @TraceIdOut, 109, 41, @On
exec sp_trace_setevent @TraceIdOut, 109, 42, @On
exec sp_trace_setevent @TraceIdOut, 109, 43, @On
exec sp_trace_setevent @TraceIdOut, 110, 6, @On
exec sp_trace_setevent @TraceIdOut, 110, 7, @On
exec sp_trace_setevent @TraceIdOut, 110, 8, @On
exec sp_trace_setevent @TraceIdOut, 110, 9, @On
exec sp_trace_setevent @TraceIdOut, 110, 10, @On
exec sp_trace_setevent @TraceIdOut, 110, 11, @On
exec sp_trace_setevent @TraceIdOut, 110, 14, @On
exec sp_trace_setevent @TraceIdOut, 110, 21, @On
exec sp_trace_setevent @TraceIdOut, 110, 23, @On
exec sp_trace_setevent @TraceIdOut, 110, 27, @On
exec sp_trace_setevent @TraceIdOut, 110, 35, @On
exec sp_trace_setevent @TraceIdOut, 110, 38, @On
exec sp_trace_setevent @TraceIdOut, 110, 39, @On
exec sp_trace_setevent @TraceIdOut, 110, 40, @On
exec sp_trace_setevent @TraceIdOut, 110, 41, @On
exec sp_trace_setevent @TraceIdOut, 111, 6, @On
exec sp_trace_setevent @TraceIdOut, 111, 7, @On
exec sp_trace_setevent @TraceIdOut, 111, 8, @On
exec sp_trace_setevent @TraceIdOut, 111, 9, @On
exec sp_trace_setevent @TraceIdOut, 111, 10, @On
exec sp_trace_setevent @TraceIdOut, 111, 11, @On
exec sp_trace_setevent @TraceIdOut, 111, 14, @On
exec sp_trace_setevent @TraceIdOut, 111, 21, @On
exec sp_trace_setevent @TraceIdOut, 111, 23, @On
exec sp_trace_setevent @TraceIdOut, 111, 27, @On
exec sp_trace_setevent @TraceIdOut, 111, 35, @On
exec sp_trace_setevent @TraceIdOut, 111, 38, @On
exec sp_trace_setevent @TraceIdOut, 111, 40, @On
exec sp_trace_setevent @TraceIdOut, 111, 41, @On
exec sp_trace_setevent @TraceIdOut, 112, 6, @On
exec sp_trace_setevent @TraceIdOut, 112, 7, @On
exec sp_trace_setevent @TraceIdOut, 112, 8, @On
exec sp_trace_setevent @TraceIdOut, 112, 9, @On
exec sp_trace_setevent @TraceIdOut, 112, 10, @On
```

```
exec sp_trace_setevent @TraceIdOut, 112, 11, @On
exec sp_trace_setevent @TraceIdOut, 112, 14, @On
exec sp_trace_setevent @TraceIdOut, 112, 23, @On
exec sp_trace_setevent @TraceIdOut, 112, 27, @On
exec sp_trace_setevent @TraceIdOut, 112, 35, @On
exec sp_trace_setevent @TraceIdOut, 112, 38, @On
exec sp_trace_setevent @TraceIdOut, 112, 40, @On
exec sp_trace_setevent @TraceIdOut, 112, 41, @On
exec sp_trace_setevent @TraceIdOut, 113, 1, @On
exec sp_trace_setevent @TraceIdOut, 113, 6, @On
exec sp_trace_setevent @TraceIdOut, 113, 7, @On
exec sp_trace_setevent @TraceIdOut, 113, 8, @On
exec sp_trace_setevent @TraceIdOut, 113, 9, @On
exec sp_trace_setevent @TraceIdOut, 113, 10, @On
exec sp_trace_setevent @TraceIdOut, 113, 11, @On
exec sp_trace_setevent @TraceIdOut, 113, 14, @On
exec sp_trace_setevent @TraceIdOut, 113, 19, @On
exec sp_trace_setevent @TraceIdOut, 113, 23, @On
exec sp_trace_setevent @TraceIdOut, 113, 27, @On
exec sp_trace_setevent @TraceIdOut, 113, 35, @On
exec sp_trace_setevent @TraceIdOut, 113, 40, @On
exec sp_trace_setevent @TraceIdOut, 113, 41, @On
exec sp_trace_setevent @TraceIdOut, 114, 1, @On
exec sp_trace_setevent @TraceIdOut, 114, 6, @On
exec sp_trace_setevent @TraceIdOut, 114, 7, @On
exec sp_trace_setevent @TraceIdOut, 114, 8, @On
exec sp_trace_setevent @TraceIdOut, 114, 9, @On
exec sp_trace_setevent @TraceIdOut, 114, 10, @On
exec sp_trace_setevent @TraceIdOut, 114, 11, @On
exec sp_trace_setevent @TraceIdOut, 114, 14, @On
exec sp_trace_setevent @TraceIdOut, 114, 19, @On
exec sp_trace_setevent @TraceIdOut, 114, 23, @On
exec sp_trace_setevent @TraceIdOut, 114, 27, @On
exec sp_trace_setevent @TraceIdOut, 114, 35, @On
exec sp_trace_setevent @TraceIdOut, 114, 40, @On
exec sp_trace_setevent @TraceIdOut, 114, 41, @On
exec sp_trace_setevent @TraceIdOut, 115, 1, @On
exec sp_trace_setevent @TraceIdOut, 115, 6, @On
exec sp_trace_setevent @TraceIdOut, 115, 7, @On
exec sp_trace_setevent @TraceIdOut, 115, 8, @On
exec sp_trace_setevent @TraceIdOut, 115, 9, @On
exec sp_trace_setevent @TraceIdOut, 115, 10, @On
exec sp_trace_setevent @TraceIdOut, 115, 11, @On
exec sp_trace_setevent @TraceIdOut, 115, 14, @On
exec sp_trace_setevent @TraceIdOut, 115, 21, @On
exec sp_trace_setevent @TraceIdOut, 115, 23, @On
exec sp_trace_setevent @TraceIdOut, 115, 27, @On
exec sp_trace_setevent @TraceIdOut, 115, 35, @On
exec sp_trace_setevent @TraceIdOut, 115, 40, @On
exec sp_trace_setevent @TraceIdOut, 115, 41, @On
```

```
exec sp_trace_setevent @TraceIdOut, 116, 1, @On
exec sp_trace_setevent @TraceIdOut, 116, 6, @On
exec sp_trace_setevent @TraceIdOut, 116, 7, @On
exec sp_trace_setevent @TraceIdOut, 116, 8, @On
exec sp_trace_setevent @TraceIdOut, 116, 9, @On
exec sp_trace_setevent @TraceIdOut, 116, 10, @On
exec sp_trace_setevent @TraceIdOut, 116, 11, @On
exec sp_trace_setevent @TraceIdOut, 116, 14, @On
exec sp_trace_setevent @TraceIdOut, 116, 23, @On
exec sp_trace_setevent @TraceIdOut, 116, 27, @On
exec sp_trace_setevent @TraceIdOut, 116, 35, @On
exec sp_trace_setevent @TraceIdOut, 116, 40, @On
exec sp_trace_setevent @TraceIdOut, 116, 41, @On
exec sp_trace_setevent @TraceIdOut, 117, 6, @On
exec sp_trace_setevent @TraceIdOut, 117, 7, @On
exec sp_trace_setevent @TraceIdOut, 117, 8, @On
exec sp_trace_setevent @TraceIdOut, 117, 9, @On
exec sp_trace_setevent @TraceIdOut, 117, 10, @On
exec sp_trace_setevent @TraceIdOut, 117, 11, @On
exec sp_trace_setevent @TraceIdOut, 117, 14, @On
exec sp_trace_setevent @TraceIdOut, 117, 21, @On
exec sp_trace_setevent @TraceIdOut, 117, 23, @On
exec sp_trace_setevent @TraceIdOut, 117, 27, @On
exec sp_trace_setevent @TraceIdOut, 117, 41, @On
exec sp_trace_setevent @TraceIdOut, 118, 1, @On
exec sp_trace_setevent @TraceIdOut, 118, 14, @On
exec sp_trace_setevent @TraceIdOut, 118, 21, @On
exec sp_trace_setevent @TraceIdOut, 118, 23, @On
exec sp_trace_setevent @TraceIdOut, 118, 27, @On
exec sp_trace_setevent @TraceIdOut, 118, 28, @On
exec sp_trace_setevent @TraceIdOut, 118, 34, @On
exec sp_trace_setevent @TraceIdOut, 118, 35, @On
exec sp_trace_setevent @TraceIdOut, 118, 40, @On
-- Tercero, define los filtros (se recomienda excluir los eventos de select y los
comandos que se requiere auditar para limitar la cantidad de eventos
registrados):
-- exec sp_trace_setfilter trace_id,column_id,logical_oper,comp_oper,value
--filtro de aplicaciones propios del SQL Server
exec sp_trace_setfilter @TraceIdOut, 60, 0, 0, 0 -- AND IsSystem = 0
--se incluyen los
-- Cuarto, activa/desactiva la traza:
exec sp_trace_setstatus @TraceIdOut,@On_status
end
GO
exec sp_procoption N'traza_si', N'startup', N'true'
GO
```

SAP ASE 16 SP01

sp_audit "all", "sso_role", "all", "on"
sp_audit "all", "sa_role", "all", "on"
sp_audit "cmdtext",”[login del usuario]", "all",”on” (*)

(*) esta sentencia se ejecuta para cada usuario al que se le habilita el registro de eventos.

Teradata 13.10

BEGIN QUERY LOGGING ACCOUNT='[cuenta del usuario]'; (*)
(*) esta sentencia se ejecuta para cada usuario al que se le habilita el registro de eventos.

Anexo XVI: Cuadro con las opciones de configuración de los sistemas de gestión de base de datos relacional

TERADATA 13.10

Instalación	Script de instalación	N/A
	Privilegios para ejecutar script de instalación	N/A
Configuración	Comandos de configuración	BEGIN QUERY LOGGING
		END QUERY LOGGING
		REPLACE QUERY LOGGING
	Privilegios para configurar la auditoria	Execute en DBC.DBQLAccessMacro
	Nivel de auditoria	Usuario Grupo de usuarios Cuenta Lista de cuentas Aplicación
	Configuración en línea	SI
	Repositorio de eventos	Tablas: DBQLExplainTbl DBQLogTbl DBQLObjTbl DBQLSQLTbl DBQLStepTbl DBQLSummaryTbl DBQLXMLTbl
	Gestión de almacenamiento y depuración de registros de eventos	Uso de tablas temporales e históricas DBQLOGTBL_TMP DBQLSQLTBL_TMP DBQLOBJTBL_TMP DBQLSummaryTBL_TMP DBQLOGTBL_HST DBQLSQLTBL_HST DBQLOBJTBL_HST

		DBQLOBJTBL_SUM DBQLSummaryTBL_HST
	Posibilidad de agregar registros	NO
	Consulta de opciones de auditoria habilitadas	Vista DBC.DBQLRulesV Comando SHOW QUERY LOGGING

SAP ASE 16.0 SP01

Instalación	Script de instalación	auditinit (para Unix) instsecu (para Windows)
	Privilegios para ejecutar script de instalación	Rol SA
Configuración	Comandos de configuración	sp_configure sp_audit
	Privilegios para configurar la auditoria	Rol SSO
	Nivel de auditoria	Servidor Base de datos Objeto Usuario
	Configuración en línea	SI
	Repositorio de eventos	Base de datos Sybsecurity y tablas Sysaudits
	Gestión de almacenamiento y depuración de registros de eventos	Uso de procedimientos almacenados sp_addthreshold y sp_configure
	Posibilidad de agregar registros	SI (procedimiento almacenado sp_addauditrecord)

	Consulta de opciones de auditoria habilitadas	Tabla sysauditoptions o procedimiento almacenado sp_displayaudit

SQL SERVER 12 – Modalidad C2

Instalación	Script de instalación	N/A
	Privilegios para ejecutar script de instalación	N/A
Configuración	Comandos de configuración	Procedimiento almacenado sp_configure
	Privilegios para configurar la auditoria	Rol sysadmin
	Nivel de auditoria	Servidor
	Configuración en línea	NO
	Repositorio de eventos	Archivos con extensión trc
	Gestión de almacenamiento y depuración de registros de eventos	Tareas operativas
	Posibilidad de agregar registros	NO
	Consulta de opciones de auditoria habilitadas	Tabla sys.configurations

SQL SERVER 12 – Common Criteria Compliance

Instalación	Script de instalación	Script de configuración de nivel 4 de Common Criteria Evaluation (EAL4+)
	Privilegios para ejecutar script de instalación	Permisos para ejecutar el script

Configuración	Comandos de configuración	Procedimiento almacenado sp_configure
	Privilegios para configurar la auditoria	Roles sysadmin y serveradmin
	Nivel de auditoria	Servidor
	Configuración en línea	NO
	Repositorio de eventos	Archivos con extensión trc
	Gestión de almacenamiento y depuración de registros de eventos	Tareas operativas
	Posibilidad de agregar registros	NO
	Consulta de opciones de auditoria habilitadas	Tabla sys.configurations

SQL SERVER 12 – Trigger

Instalación	Script de instalación	N/A
	Privilegios para ejecutar script de instalación	N/A
Configuración	Comandos de configuración	create trigger
		alter trigger
		drop trigger
	Privilegios para configurar la auditoria	Permiso de Control Server sobre el servidor y rol sysadmin para detener la ejecución del trigger

	Nivel de auditoria	Usuario
	Configuración en línea	SI
	Repositorio de eventos	Tablas definidas por el usuario
	Gestión de almacenamiento y depuración de registros de eventos	Tareas operativas
	Posibilidad de agregar registros	SI
	Consulta de opciones de auditoria habilitadas	Revisión operativa/manual de los triggers configurados

SQL SERVER 12 - SQL Trace

Instalación	Script de instalación	N/A
	Privilegios para ejecutar script de instalación	N/A
Configuración	Comandos de configuración	Procedimientos almacenados sp_trace_setevent sp_trace_setfilter sp_trace_create sp_trace_generateevent sp_trace_setstatus
	Privilegios para configurar la auditoria	Permiso de Alter Trace
	Nivel de auditoria	Servidor
	Configuración en línea	NO
	Repositorio de eventos	Archivos con extensión trc o una tabla
	Gestión de almacenamiento y depuración de registros de eventos	Definición de los parámetros: Máximo tamaño de cada archivo (MB) Rotación al siguiente archivo al alcanzar el tamaño maximo del

		archivo
	Posibilidad de agregar registros	SI (procedimiento almacenado sp_trace_generateevent)
	Consulta de opciones de auditoria habilitadas	Tabla sys.traces

SQL SERVER 12 - SQL Audit

Instalación	Script de instalación	N/A
	Privilegios para ejecutar script de instalación	N/A
Configuración	Comandos de configuración	Comandos Create Server Audit Especification Create Database Audit Especification
	Privilegios para configurar la auditoria	Rol sysadmin Privilegios: CONTROL SERVER VIEW SERVER STATE ALTER ANY AUDIT VIEW AUDIT STATE
	Nivel de auditoria	Servidor Base de datos
	Configuración en línea	NO
	Repositorio de eventos	Registro de eventos de Windows o archivos externos a la base de datos
	Gestión de almacenamiento y depuración de registros de eventos	Definición de los parámetros: Demora en cola (en milisegundos) Máximo número de archivos a retener Máximo tamaño de cada archivo (MB) Espacio del disco reservado para los archivos de la auditoría Máxima cantidad de archivos

	Posibilidad de agregar registros	SI (procedimiento almacenado sp_audit_write)
	Consulta de opciones de auditoría habilitadas	Vistas Sys.dm_server_audits_status Sys.dm_audit_actions Sys.dm_audits_class_type_map Sys.server_audits Sys.server_audit_specifications_details Sys.database_audit_specifications Sys.database_audit_specifications_details Sys.server_audit_specifications

ORACLE 12 C – Básica

Instalación	Script de instalación	N/A
	Privilegios para ejecutar script de instalación	N/A
Configuración	Comandos de configuración	Comandos
		audit_trail audit noaudit
	Privilegios para configurar la auditoria	Privilegio ALTER SYSTEM Privilegio AUDIT ANY o dueño del objeto Privilegio AUDIT ANY o dueño del objeto
	Nivel de auditoria	Servidor Base de datos Sentencia SQL Objeto
	Configuración en línea	SI (a partir de la versión 11 g r2)

	Repositorio de eventos	Tablas DBA_AUDIT_TRAIL DBA_AUDIT_STATEMENT DBA_AUDIT_SESSION DBA_AUDIT_OBJECT DBA_AUDIT_EXISTS o registro de eventos del sistema operativo o archivos de formato XML (vista V$XML_AUDIT_TRAIL)
	Gestión de almacenamiento y depuración de registros de eventos	Tareas operativas
	Posibilidad de agregar registros	NO
	Consulta de opciones de auditoria habilitadas	Comando: Show parameter audit Vistas: All_def_audit_opts Dba_stmt_audit_opts Dba_priv_audit_opts Dba_obj_audit_opts

ORACLE 12 C - Auditar a Sysdba y a los usuarios Sysoper

Instalación	Script de instalación	N/A
	Privilegios para ejecutar script de instalación	N/A
Configuración	Comandos de configuración	Parámetro: Audit_sys_operations
	Privilegios para configurar la auditoria	Privilegio ALTER SYSTEM
	Nivel de auditoria	Usuario SYS
	Configuración en línea	SI (a partir de la versión 11 g r2)

	Repositorio de eventos	Registro de eventos del sistema operativo o archivos de formato XML (vista V$XML_AUDIT_TRAIL)
	Gestión de almacenamiento y depuración de registros de eventos	Tareas operativas
	Posibilidad de agregar registros	NO
	Consulta de opciones de auditoria habilitadas	Comando: Show parameter audit

ORACLE 12 C - Funcionalidad FGA

Instalación	Script de instalación	DBMS_FGA (versión 10 g) DBMS_AUDIT_MGMT (a partir de la versión 11g r2)
	Privilegios para ejecutar script de instalación	Privilegio de ejecución del paquete DBMS_FGA Privilegio de ejecución del paquete DBMS_AUDIT_MGMT
Configuración	Comandos de configuración	Comandos DBMS_FGA.ADD_POLICY DBMS_FGA.ENABLE_POLICY DBMS_FGA.DISABLE_POLICY DBMS_FGA.DROP_POLICY
	Privilegios para configurar la auditoria	Privilegio de ejecución del paquete DBMS_FGA Privilegio de ejecución del paquete DBMS_AUDIT_MGMT
	Nivel de auditoria	Sentencias insert, delete, update y select
	Configuración en línea	SI

	Repositorio de eventos	Tabla DBA_FGA_AUDIT_TRAIL
	Gestión de almacenamiento y depuración de registros de eventos	Tareas operativas
	Posibilidad de agregar registros	NO
	Consulta de opciones de auditoria habilitadas	Comando: Desc DBA_AUDIT_POLICIES

ORACLE 12 C - Auditoria unificada

Instalación	Script de instalación	Libreria: make -f ins_rdbms.mk uniaud_on ioracle
	Privilegios para ejecutar script de instalación	Privilegio de ejecución del paquete ins_rdbms.mk uniaud_on
Configuración	Comandos de configuración	Comandos CREATE AUDIT POLICY AUDIT POLICY
	Privilegios para configurar la auditoria	Privilegio AUDIT SYSTEM o rol AUDIT_ADMIN
	Nivel de auditoría	Usuarios Roles Privilegios Acciones sobre objetos Aplicación Oracle Database Real Application Security, Oracle Recovery Manager, Oracle Data Mining, Oracle Data Pump, Oracle SQL*Loader direct path events, Oracle Database Vault y Oracle Label Security

	Configuración en línea	SI
	Repositorio de eventos	Vista Unified_audit_trail
	Gestión de almacenamiento y depuración de registros de eventos	Paquete DBMS_AUDIT_MGMT Tareas operativas
	Posibilidad de agregar registros	NO
	Consulta de opciones de auditoría habilitadas	Vista v$OPTION Vista AUDIT_UNIFIED_POLICIES

Anexo XVII: Cuadro comparativo del análisis de los registros de eventos de auditoria en los sistemas de gestión de base de datos relacional

TERADATA 13.10

Mecanismo para el análisis de eventos	Consultas de select sobre las tablas: DBQLogTbl DBQLExplainTBL DBQLObjTbl DBQLSQLTbl DBQLSteepTbl DBQLSummaryTbl DBQLXMLTbl
Privilegios	Permisos de ejecución de select sobre las tablas descriptas en la columna anterior DBQLogTbl DBQLExplainTBL DBQLObjTbl DBQLSQLTbl DBQLSteepTbl DBQLSummaryTbl DBQLXMLTbl

Análisis de eventos en DBQLogTbl

Análisis	Descripción	Campo
¿Quién?	Número de identificación único del usuario	UserID
	La cadena de caracteres de la cuenta al momento que empezó a ejecutarse la sentencia	AcctString
	El nombre de la cuenta extendida bajo la cual la consulta esta ejecutándose si es invocada.	ExpandAcctString
	Identificador único del origen del inicio de sesión	LogicalHostID
	Origen del inicio de sesión	LogonSource
	Nombre del usuario de red bajo el cual se registra la sesión	ClientID
	La dirección IP del cliente	ClientAddr

	Nombre del perfil bajo el cual el usuario ejecuta la consulta	ProfileID
	Nombre bajo el cual la sesión fue iniciada	UserName
	El nombre del usuario de la conexión del proxy	ProxyUser
	El nombre del rol de la conexión del proxy	ProxyRole
¿Cuándo?	Fecha y hora del inicio de sesión	LogonDateTime
	Fecha y hora de ejecución de la sentencia	StartTime
	Fecha y hora del primer paso de la sentencia	FirstStepTime
	Fecha y hora del primer paquete de respuesta que se envia al host	FirstRespTime
	Fecha y hora del último cambio de estado para el administrador de carga de Teradata.	LastStateChange
¿Cómo?	Aplicación o nombre del utilitario	AppID
¿Qué?	Número total de pasos requeridos para el proceso	NumSteps
	Número total de pasos incluyendo pasos paralelos	NumStepswPar
	El máximo número de niveles que se realiza en paralelo para una consulta	MaxStepsInPar
	Número total de filas que devuelve una consulta	NumResultRows
	Total de entradas y salidas que utiliza una consulta	TotalIOCount
	El número de bytes transferidos por inserción, actualización o eliminación usando Multiload o Fastload	UtilityByteCount
	El número de filas insertadas, actualizadas o eliminadas usando Multiload o Fastload	UtilityRowCount
	Tipo de la sentencia utilizada en la consulta	StatementType
	Los primeros caracteres de la consulta. Por defecto el valor es de 200 caracteres, para ampliar este valor se debe modificar el parámetro LIMIT SQLTEXT	QueryText

	Si una sentencia DDL es solicitada, el StatementGroup reporta con el tipo: • DDL ALTER • DDL CREATE • DDL GRANT Si la sentencia tiene solamente una sentencia DML o múltiples DML del mismo tipo, StatementGroup indica el tipo.	StatementGroup
	Identificador generado internamente por la sentencia	QueryID

Análisis de eventos en DBQLExplainTBL (esta tabla se completa si la opción WITH EXPLAIN fue habilitada)

Análisis	Descripción	Campo
¿Cuándo?	Fecha y hora en que las filas fueron escritas en la base de datos	CollectTimeStamp
¿Qué?	Identificador generado internamente por la sentencia	QueryID
	Campo utilizado si el texto Explain es mayor a 64 kb y el sistema genera múltiples filas	ExpRowN
	Texto completo	ExplainText

Análisis de eventos en DBQLObjTbl (esta tabla se completa si la opción WITH OBJECTS fue habilitada)

Análisis	Descripción	Campo
¿Cuándo?	Fecha y hora en que las filas fueron escritas en la base de datos	CollectTimeStamp
¿Qué?	Identificador generado internamente por la sentencia	QueryID
	Nombre de la base de datos que posee el objeto de destino	ObjectDatabaseName
	Nombre de la tabla o vista	ObjectTableName
	Nombre de la columna	ObjectColumnName
	Número de identificación único del objeto	ObjectID
	Número de la columna o índice secundario	ObjectNum

	Código de caracteres que representa al objeto	ObjectType
	Número de veces que el objeto fue accedido	FreqofUse
	Describe el uso del objeto	TypeOfUse

Análisis de eventos en DBQLSQLTbl (esta tabla se completa si la opción WITH SQL fue habilitada)

Análisis	Descripción	Campo
¿Cuándo?	Fecha y hora en que las filas fueron escritas en la base de datos	CollectTimeStamp
¿Qué?	Identificador generado internamente por la sentencia	QueryID
	Número de fila de la sentencia	SQLRowNo
	Campo de aproximadamente 32000 caracteres	SQLTextInfo

Análisis de eventos en DBQLSteepTbl (esta tabla se completa si la opción WITH STEPINFO fue habilitada)

Análisis	Descripción	Campo
¿Cuándo?	Fecha y hora en que las filas fueron escritas en la base de datos	CollectTimeStamp
	Fecha y hora cuando el paso fue enviado al AMP	StepStartTime
	Fecha y hora cuando el paso retorno del AMP	StepStopTime
	Tiempo estimado para el procesamiento determinado por el Optimizador	EstProcTime
	Un tiempo de CPU estimado en milisegundos para el paso determinado por el Optimizador	EstCPUCost
¿Qué?	Identificador generado internamente por la sentencia	QueryID
	Número de paso. Si esta fila es para un paso paralelo, el número se repite.	StepLev1Num
	Si esta fila es para un paso paralelo, este es el número de segundo nivel del paso.	StepLev2Num
	Abreviación de un nombre usado internamente para identificar el paso. Por ejemplo: DEL para un paso DELETE.	StepName
	CPU utilizado por el paso	

Uso de I/O del paso	CPUTime
Cantidad de filas estimadas por el Optimizador	IOCount
Si el nombre del paso es MRM (filas múltiples) o EXE (multiload) este campo corresponde al número de filas insertadas. Para todos los otros pasos, el RowCount es el número actual de filas retornadas por el paso.	EstRowCount
Si el nombre del paso es MRM (filas múltiples) o EXE (multiload) este campo corresponde al número de filas actualizadas.	RowCount
Si el nombre del paso es LFI (Fastload) RowCount es el número de filas cargadas.	RowCount2
Si el nombre del paso es EXE (multiload) este campo corresponde al número de filas eliminadas	RowCount3
El número de AMPs involucrado con el paso	NumofActiveAMPs
El máximo tiempo de CPU utilizado de AMP en el paso	MaxAmpCPUTime
El número de AMP con el máximo CPU utilizado por el paso	MaxCPUAmpNumber
El mínimo tiempo de CPU utilizado de AMP en el paso	MinAmpCPUTime
Cantidad de I/O del mas alto I/O utilizado de AMP en el paso	MaxAmpIO
El número de AMP con el mas alto uso de I/O para el paso	MaxIOAmpNumber
Cantidad de I/O del menor I/O de AMP utilizado en la consulta	MinAmpIO
El número de bytes de spool utilizado por el paso	SpoolUsage
El mas alto uso de spool sobre un AMP	MaxAMPSpool
Número de AMP con un alto uso de spool	MaxSpoolAmpNumber
El mas bajo uso de spool sobre un AMP	MinAMPSpool
La definición de workload en efecto para el paso	StepWD
El número de secuencia de logon utilizado por la utilidad load	LSN

	El número de identificación de la tabla para la utilidad. Este campo es siempre cero	UtilityTableId
	Número de filas con filas comprimidas	RowsWComprColumns
	Un tiempo estimado de servicio en milisegundos para la I/O del paso..	EstIOCost
	Un tiempo estimado de BYNET del tiempo de servicio en milisegundos para el paso.	EstNetCost
	Un estimado de otros costos para el paso.	EstHRCost
	Tiempo AMP CPU normalizado para sistemas coexistentes	CPUTimeNorm
	Tiempo máximo de CPU normalizado por AMP	MaxAmpCPUTimeNorm
	Número de AMP con el tiempo máximo normalizado de CPU para sistemas co-existentes	MaxCPUAmpNumberNorm
	Tiempo mínimo de CPU normalizado por AMP	MinAmpCPUTimeNorm

Análisis de eventos en DBQLSummaryTbl (esta tabla se completa si la opción SUMMARY O TRESHOLD fue habilitada)

Análisis	Descripción	Campo
¿Quién?	Número de identificación único del usuario	UserID
	La cadena de caracteres de la cuenta al momento que empezó a ejecutarse la sentencia	AcctString
	Número de identificación único del origen del inicio de sesión de la consulta registrada. El valor cero indica una sesión interna.	LogicalHostID
	Número de identificación del cliente bajo el cual la consulta se ejecuta	ClientID
	Número de dirección ip del cliente bajo el cual la consulta se ejecuta	ClientAddr
	Número de identificación del perfil bajo el cual el usuario ejecuta la consulta	ProfileID
	Número de identificación de la sesión en la cual se empezó a ejecutar la consulta.	SessionID

¿Cuándo?	Fecha y hora en que las filas fueron escritas en la base de datos	CollectTimeStamp
¿Cómo?	Aplicación o nombre del utilitario	AppID
¿Qué?	Número de consultas que se ejecutaron los últimos 10 minutos	QueryCount
	El criterio del umbral es el siguiente: • C = segundos AMP CPU • H = centésimas de segundo transcurridos • I = cantidad de entradas/ salidas • N = segundos de AMP CPU normalizados • S = tiempo en segundos transcurridos.	ValueType
	Total del tiempo de ejecución de la consulta	QuerySeconds
	Cantidad total de entradas y salidas	TotalIOCount
	Tiempo total de AMP CPU	AMPCPUTime
	Tiempo de AMP CPU normalizado para sistemas coexistentes únicamente.	ParserCPUTime
	Tiempo de CPU normalizado para el análisis de las consultas	ParserCPUTimeNorm
	El valor mas alto para la opción SUMMARY - Cero para la opción THRESHOLD. - Si los modificadores CPUTIME or IOCOUNT son utilizados luego este valor es el mas alto entre segundos en CPU o cantidad de entradas y salidas por usuario.	HighHist
	El menor valor para la opción SUMMARY - Para la opción THRESHOLD el valor es el tiempo de umbral configurado para el usuario. El tiempo por defecto es 5. - Si los modificadores CPUTIME or IOCOUNT son utilizados luego este valor es el menor entre segundos en CPU o cantidad de entradas y salidas por usuario.	LowHist

Análisis de eventos en DBQLXMLTbl (esta tabla se completa si la opción WITH XMLPLAN fue habilitada)

Análisis	Descripción	Campo
¿Cuándo?	Fecha y hora en que las filas fueron escritas en la base de datos	CollectTimeStamp
¿Qué?	Identificador único generado internamente para la consulta.	QueryID
	Número en una secuencia de las filas que constituyen un plan	XMLRowNo
	Plan XML	XMLTextInfo

SAP ASE 16.0 SP01

Mecanismo para el análisis de eventos	Consultas de select sobre tablas sysaudits
Privilegios	Rol SSO

Análisis de eventos en tablas syaudits

Análisis	Descripción	Campo
¿Quién?	Nombre del login correspondiente al suid	loginname
	Número de identificación del login del usuario que realizó el evento	suid
	Información adicional del evento registrado (dirección ip del cliente)	extrainfo
¿Cuándo?	Fecha y hora de ocurrencia del evento	eventtime
¿Qué?	Información adicional del evento registrado	extrainfo
¿Cómo?	Codigo del evento	event
	Brinda mayor información sobre el evento	eventmod
	Número de identificación del proceso que causo que se registre el evento	spid
	Número de secuencia del registro dentro de un evento	sequence
	Número de identificación de la base de datos en la cual ocurrió el evento o en la cual el objeto, procedimiento almacenado o trigger reside	dbid

	Número de identificación del objeto, procedimiento almacenado o trigger al que se accedió.	objid
	Número de identificación de la transacción del evento registrado	xactid
	Nombre de la base de datos correspondiente al dbid	dbname
	Nombre del objeto correspondiente al objid	objname
	Nombre del dueño del objid	objowner
	Número de identificación del nodo del servidor en el cluster	Nodeid
	Información adicional del evento registrado	extrainfo

SQL SERVER 12 - Modalidad C2, Common Criteria Compliance y SQL Trace

Mecanismo para el análisis de eventos	Herramienta SQL Profiler o uso de la función del sistema sys.fn_trace_gettable
Privilegios	Para utilizar la función sys.fn_trace_gettable se requiere el privilegio de ALTER TRACE sobre el servidor. Para emplear SQL Profiler para la lectura de los archivos de extensión .trc no se requieren permisos en SQL

Análisis de eventos en los archivos de extensión trc

Análisis	Descripción	Campo
¿Quién?	Número de identificación asignado por la computadora al proceso donde la aplicación del cliente se ejecuta.	ClientProcessID
	Nombre del usuario de SQL Server del cliente	DBUserName
	Nombre de la computadora sobre la cual el cliente esta corriendo	Host Name
	Nombre del login del usuario	LoginName
	Número de identificación de seguridad (SID) del usuario logeado	LoginSid
	Dominio de Microsoft Windows NT® 4.0 o Windows 2000 al que el usuario pertenece	NT Domain Name
	Nombre del usuario de Windows NT 4.0 o Windows 2000.	NT User Name

	Nombre del rol de la aplicación que está habilitado	RoleName
	Nombre del login específico	TargetLoginName
	El SID del login específico	TargetLoginSid
	Para acciones asociadas a un usuario de base de datos, por ejemplo: otorgar permisos a un usuario.	TargetUserName
¿Cuándo?	Cantidad de tiempo, en milisegundos tomados por el evento	Duration
	Tiempo en el cual el evento finalizó.	End Time
	Tiempo de inicio del evento.	Start Time
¿Qué?	Nombre de la aplicación cliente que creo la conexión a una instancia de SQL Server	Application Name
¿Cómo?	Tipo de la clase del evento capturado.	EventClass
	Tipo de la subclase del evento, provee información adicional de cada clase de evento	EventSubClass
	Número de identificación asignado al objeto.	Object ID
	Nombre del objeto que se empezó a referenciar.	ObjectName
	Valor que representa el tipo de objeto involucrado en el evento. Este valor corresponde a la columna type en sysobjects.	ObjectType
	Número entero que representa el tipo de permiso verificado. Los valores posibles son: 1 = SELECT ALL 2 = UPDATE ALL 4 = REFERENCES ALL 8 = INSERT 16 = DELETE 32 = EXECUTE (procedures only) 4096 = SELECT ANY (at least one column) 8192 = UPDATE ANY 16384 = REFERENCES ANY	Permissions
	Número de identificación del proceso asignado por SQL Server para el proceso asociado con el cliente.	SPID
	Equivalente a un código de estado de error	State

	Valor de resultado del evento: 1: exitoso, los permisos verificados exitosamente. 2: error /falla al verificar los permisos	Success
	Texto descriptivo del evento capturado en la traza	TextData
	Número de identificación asignado a la transacción	Transaction ID

SQL SERVER 12 - SQL Audit

Mecanismo para el análisis de eventos	Consulta al archivos a través de la función sys.fn_get_audit_file
Privilegios	Privilegio de CONTROL SERVER

Análisis de eventos de SQL Audit

Análisis	**Descripción**	**Campo**
¿Quién?	Número de identificación de la sesión sobre la cual el evento ocurrió	session_id
	Número de identificación del contexto de login que realizó la acción	server_principal_id
	Número de identificación del contexto del usuario de base de datos que realizó la acción	database_principal_id
	Login actual	server_principal_name
	SID del login actual	server_principal_sid
	Usuario actual	database_principal_name
¿Cuándo?	Fecha y hora del registro del evento	event_time
¿Qué?	N/A	N/A
¿Cómo?	Valor que representa el tipo de objeto involucrado en el evento. Este valor corresponde a la columna type en sysobjects.	ObjectType

	Número entero que representa el tipo de permiso verificado. Los valores posibles son: 1 = SELECT ALL 2 = UPDATE ALL 4 = REFERENCES ALL 8 = INSERT 16 = DELETE 32 = EXECUTE (procedures only) 4096 = SELECT ANY (at least one column) 8192 = UPDATE ANY 16384 = REFERENCES ANY	Permissions
	Número de identificación del proceso asignado por SQL Server para el proceso asociado con el cliente.	SPID
	Equivalente a un código de estado de error	State
	Valor de resultado del evento: 1: exitoso, los permisos verificados exitosamente. 2: error /falla al verificar los permisos	Success
	Texto descriptivo del evento capturado en la traza	TextData
	Número de identificación asignado a la transacción	Transaction ID
	Número de identificación de la acción	action_id
	Indica el resultado de la acción	Succeeded
	En algunas acciones, estos son los permisos que fueron otorgados, denegados o revocados	permission_bitmask
	Servidor principal donde se realizan las operaciones GRANT/DENY/REVOKE	target_server_principal_id
	Base de datos donde se realizan las operaciones GRANT/DENY/REVOKE	target_database_principal_id
	En número de identificación de la entidad donde ocurrió la auditoria	object_id
	El tipo de entidad auditable sobre la que ocurrió el evento a auditar	class_type

	Servidor principal por sesión.	session_server_principal_name
	Nombre de la instancia del servidor donde la auditoria ocurrió	server_instance_name
	El contexto de la base de datos en la cual la acción ocurrió	database_name
	El contexto del esquema en la cual la acción ocurrió	schema_name
	El nombre de la entidad en la cual la auditoria ocurrió	object_name
	Sentencia TSQL	statement
	Información única que se aplica solamente a un simple evento retornado un XML	additional_information
	Usuario definido pasado como un argumento en el procedimiento almacenado **sp_audit_write**	user_defined_event_id
	Utilizado para cualquier registro extra de información que el usuario quiera guardar en el log de auditoria, utilizando el procedimiento almacenado **sp_audit_write**	user_defined_information
	Secuencia del registro dentro de un registro de auditoria cuando esta fue muy extensa.	sequence_number

SQL SERVER 12 – Resgistro de eventos del sistema operativo (seguridad o aplicación)

Mecanismo para el análisis de eventos	Consulta al registro de eventos del sistema operativo (seguridad o aplicación)
Privilegios	Permiso de lectura en el registro de eventos del sistema operativo

Análisis de eventos del registro de eventos del sistema operativo

Análisis	**Descripción**
¿Quién? ¿Cuándo? ¿Qué? ¿Cómo?	La información se guarda en eventos con el número de identificación 33205. En el detalle de dicho evento se encuentran los mismos campos descriptos para la funcionalidad de SQL Audit

Oracle 12 C – Registro de eventos en tablas DBA

Mecanismo para el análisis de eventos	Consultas de select sobre las tablas DBA_AUDIT_TRAIL DBA_AUDIT_STATEMENT DBA_AUDIT_SESSION DBA_AUDIT_OBJECT DBA_AUDIT_EXISTS
Privilegios	Permisos de ejecucion de select sobre las tablas
	DBA_AUDIT_TRAIL DBA_AUDIT_STATEMENT DBA_AUDIT_SESSION DBA_AUDIT_OBJECT DBA_AUDIT_EXISTS

Análisis de eventos de DBA_AUDIT_TRAIL

Análisis	**Descripción**	**Campo**
¿Quién?	Nombre del usuario que inicia sesión en el sistema operativo	OS_USERNAME
	Nombre del usuario	USERNAME
	Nombre de la máquina o host del cliente	USERHOST
	Identificador de la terminal del usuario	TERMINAL
	Número de identificación para cada sesión de Oracle	SESSIONID
	Identificador del cliente en cada sesión de Oracle	CLIENT_ID
	Número serial de la sesión de proxy, si un usuario inicio sesión a través del mecanismo de proxy	PROXY_SESSIONID
	Identificador global del usuario	GLOBAL_UID
¿Cuándo?	Fecha y hora de la creación en el registro de eventos	TIMESTAMP
	Fecha y hora del cierre de sesión	LOGOFF_TIME
	Tiempo de la creación de la entrada del registro de evento de auditoria	EXTENDED_TIMESTAMP
¿Qué?	N/A	N/A
¿Cómo?	Creador del objeto afectado en la acción	OWNER
	Nombre del objeto afectado por la acción	OBJ_NAME
	Código numérico del tipo de	ACTION

	acción	
	Nombre de la acción correspondiente al código numérico	ACTION_NAME
	Dueño del objeto nombrado en la columna NEW_NAME	NEW_OWNER
	Nuevo nombre del objeto	NEW_NAME
	Privilegios otorgados o revocados por un GRANT o REVOKE	OBJ_PRIVILEGE
	Privilegios del sistema otorgados o revocados por un GRANT o REVOKE	SYS_PRIVILEGE
	Indica que roles o privilegios del sistema fueron otorgados con la opción ADMIN	$
	Nombre de lo otorgado especificamente en una sentencia GRANT o REVOKE	GRANTEE
	Opción de auditoria configurada con la sentencia AUDIT	AUDIT_OPTION
	Resumen de la sesión	SES_ACTIONS
	Lecturas lógicas por session	LOGOFF_LREAD
	Lecturas físicas por sesión	LOGOFF_PREAD
	Escrituras físicas por sesión	LOGOFF_LWRITE
	Bloqueos detectados durante la sesión	LOGOFF_DLOCK
	Comentarios adicionales sobre el registro de eventos, provee mayor información sobre la sentencia auditada.	COMMENT_TEXT
	Número de identificación para cada sesión de Oracle	SESSIONID
	Número de identificación para cada entrada al registro de evento de auditoria en la sesión	ENTRYID
	Número de identificación para cada sentencia que se ejecuta	STATEMENTID
	Código de error de Oracle generado por la acción	RETURNCODE
	Privilegio de sistema usado para ejecutar la acción	PRIV_USED
	Cantidad de tiempo de CPU usado por cada sesión de Oracle	SESSION_CPU
	Identificador de la transacción en la cual el objeto es accedido o modificado	TRANSACTIONID
	Datos de la variable en la consulta	SQL_BIND

	Identificador del proceso del sistema operativo del proceso de Oracle	OS_PROCESS
	Texto de SQL en la consulta	SQL_TEXT

Análisis de eventos en la tabla DBA_AUDIT_STATEMENT

Análisis	Descripción	Campo
¿Quién?	Nombre del usuario que inicia sesión en el sistema operativo	OS_USERNAME
	Nombre del usuario	USERNAME
	Nombre de la máquina o host del cliente	USERHOST
	Identificador de la terminal del usuario	TERMINAL
	Número de identificación para cada sesión de Oracle	SESSIONID
	Identificador del cliente en cada sesión de Oracle	CLIENT_ID
	Número serial de la sesión de proxy, si un usuario inicio sesión a través del mecanismo de proxy	PROXY_SESSIONID
	Identificador global del usuario	GLOBAL_UID
¿Cuándo?	Fecha y hora de la creación en el registro de eventos	TIMESTAMP
	Tiempo de la creación de la entrada del registro de evento de auditoria	EXTENDED_TIMESTAMP
¿Qué?	N/A	N/A
¿Cómo?	Creador del objeto afectado en la acción	OWNER
	Nombre del objeto afectado por la acción	OBJ_NAME
	Nombre de la acción correspondiente al código numérico.	ACTION_NAME
	Nuevo nombre del objeto	NEW_NAME
	Privilegios otorgados o revocados por un GRANT o REVOKE	OBJ_PRIVILEGE
	Privilegios del sistema otorgados o revocados por un GRANT o REVOKE	SYS_PRIVILEGE
	Indica que roles o privilegios del sistema fueron otorgados con la opción ADMIN	ADMIN_OPTION
	Nombre de lo otorgado especificamente en una sentencia	GRANTEE

	GRANT o REVOKE	
	Opción de auditoria configurada con la sentencia AUDIT	AUDIT_OPTION
	Resumen de la sesión, 16 caracteres por cada acción	SES_ACTIONS
	Comentarios adicionales	COMMENT_TEXT
	Número de identificación para cada entrada al registro de evento de auditoria en la sesión	ENTRYID
	Número de identificación para cada sentencia que se ejecuta	STATEMENTID
	Código de error de Oracle generado por la acción	RETURNCODE
	Privilegio de sistema usado para ejecutar la acción	PRIV_USED
	Cantidad de tiempo de CPU usado por cada sesión de Oracle	SESSION_CPU
	Identificador del proceso del sistema operativo del proceso de Oracle	OS_PROCESS
	Identificador de la transacción en la cual el objeto es accedido o modificado	TRANSACTIONID
	Datos de la variable en la consulta	SQL_BIND
	Texto de SQL en la consulta	SQL_TEXT

Análisis de eventos en la tabla DBA_AUDIT_SESSION

Análisis	Descripción	Campo
¿Quién?	Nombre del usuario que inicia sesión en el sistema operativo	OS_USERNAME
	Nombre del usuario	USERNAME
	Nombre de la máquina o host del cliente	USERHOST
	Identificador de la terminal del usuario	TERMINAL
	Identificador del cliente en cada sesión de Oracle	CLIENT_ID
	Número serial de la sesión de proxy, si un usuario inicio sesión a través del mecanismo de proxy	PROXY_SESSIONID
	Identificador global del usuario	GLOBAL_UID
¿Cuándo?	Fecha y hora de la creación en el registro de eventos	TIMESTAMP
	Fecha y hora que el usuario cierra sesión	LOGOFF_TIME

	Tiempo de la creación de la entrada del registro de evento de auditoria	EXTENDED_TIMESTAMP
¿Qué?	N/A	N/A
¿Cómo?	Nombre de la acción correspondiente al código numérico.	ACTION_NAME
	Lecturas lógicas para la sesión	LOGOFF_LREAD
	Lecturas físicas para la sesión	LOGOFF_PREAD
	Escrituras lógicas para la sesión	LOGOFF_LWRITE
	Bloqueos detectados durante la sesión	LOGOFF_DLOCK
	Número de identificación para cada sesión de Oracle	SESSIONID
	Código de error de Oracle generado por la acción	RETURNCODE
	Cantidad de tiempo de CPU usado por cada sesión de Oracle	SESSION_CPU
	Identificador del proceso del sistema operativo del proceso de Oracle	OS_PROCESS

Análisis de eventos en la tabla DBA_AUDIT_OBJECT

Análisis	Descripción	Campo
¿Quién?	Nombre del usuario que inicia sesión en el sistema operativo	OS_USERNAME
	Nombre del usuario	USERNAME
	Nombre de la máquina o host del cliente	USERHOST
	Identificador de la terminal del usuario	TERMINAL
	Número de identificación para cada sesión de Oracle	SESSIONID
	Identificador del cliente en cada sesión de Oracle	CLIENT_ID
	Número serial de la sesión de proxy, si un usuario inicio sesión a través del mecanismo de proxy	PROXY_SESSIONID
	Identificador global del usuario	GLOBAL_UID
¿Cuándo?	Fecha y hora de la creación en el registro de eventos	TIMESTAMP
	Tiempo de la creación de la entrada del registro de evento de auditoria	EXTENDED_TIMESTAMP
¿Qué?	N/A	N/A
¿Cómo?	Creador del objeto afectado en	OWNER

	la acción	
	Nombre del objeto afectado por la acción	OBJ_NAME
	Nombre de la acción correspondiente al código numérico.	ACTION_NAME
	Dueño del objeto nombrado en la columna NEW_NAME	NEW_OWNER
	Nuevo nombre del objeto o el nombre del objeto subrayado	NEW_NAME
	Resumen de la sesión, 16 caracteres por cada acción	SES_ACTIONS
	Comentarios adicionales	COMMENT_TEXT
	Número de identificación para cada entrada al registro de evento de auditoria en la sesión	ENTRYID
	Número de identificación para cada sentencia que se ejecuta	STATEMENTID
	Código de error de Oracle generado por la acción	RETURNCODE
	Privilegio de sistema usado para ejecutar la acción	PRIV_USED
	Cantidad de tiempo de CPU usadp por cada sesión de Oracle	SESSION_CPU
	Identificador del proceso del sistema operativo del proceso de Oracle	OS_PROCESS
	Identificador de la transacción en la cual el objeto es accedido o modificado	TRANSACTIONID
	Datos de la variable en la consulta	SQL_BIND
	Texto de SQL en la consulta	SQL_TEXT

Análisis de eventos en la tabla DBA_AUDIT_EXISTS

Análisis	Descripción	Campo
¿Quién?	Nombre del usuario que inicia sesión en el sistema operativo	OS_USERNAME
	Nombre del usuario	USERNAME
	Nombre de la máquina o host del cliente	USERHOST
	Identificador de la terminal del usuario	TERMINAL
	Identificador del cliente en cada sesión de Oracle	CLIENT_ID
	Número serial de la sesión de proxy, si un usuario inicio sesión	PROXY_SESSIONID

	a través del mecanismo de proxy	
	Identificador global del usuario	GLOBAL_UID
¿Cuándo?	Fecha y hora de la creación en el registro de eventos	TIMESTAMP
	Tiempo de la creación de la entrada del registro de evento de auditoria	EXTENDED_TIMESTAMP
¿Qué?	N/A	N/A
¿Cómo?	Creador del objeto afectado en la acción	OWNER
	Nombre del objeto afectado por la acción	OBJ_NAME
	Nombre de la acción correspondiente al código numérico.	ACTION_NAME
	Dueño del objeto nombrado en la columna NEW_NAME	NEW_OWNER
	Nuevo nombre del objeto o el nombre del objeto subrayado	NEW_NAME
	Privilegios otorgados o revocados por un GRANT o REVOKE	OBJ_PRIVILEGE
	Privilegios del sistema otorgados o revocados por un GRANT o REVOKE	SYS_PRIVILEGE
	Nombre de lo otorgado especificamente en una sentencia GRANT o REVOKE	GRANTEE
	Número de identificación para cada sesión de Oracle	SESSIONID
	Número de identificación para cada entrada al registro de evento de auditoria en la sesión	ENTRYID
	Número de identificación para cada sentencia que se ejecuta	STATEMENTID
	Código de error de Oracle generado por la acción	RETURNCODE
	Cantidad de tiempo de CPU usadp por cada sesión de Oracle	SESSION_CPU
	Identificador del proceso del sistema operativo del proceso de Oracle	OS_PROCESS
	Identificador de la transacción en la cual el objeto es accedido o modificado	TRANSACTIONID
	Datos de la variable en la consulta	SQL_BIND

	Texto de SQL en la consulta	SQL_TEXT

Oracle 12 C – Registro de eventos en archivos de formato xml o la vista V$XML_AUDIT_TRAIL

Mecanismo para el análisis de eventos	Consulta a los archivos de formato XML o la vista V$XML_AUDIT_TRAIL
Privilegios	Permiso de consulta a los archivos de formato XML o la vista V$XML_AUDIT_TRAIL

Análisis de eventos en archivos de formato XML o la vista V$XML_AUDIT_TRAIL

Análisis	Descripción	Campo
¿Quién?	Número serial de la sesión de proxy, si un usuario inicio sesión a través del mecanismo de proxy	PROXY_SESSIONID
	Identificador global del usuario	GLOBAL_UID
	Usuario de la base de datos	DB_USER
	Identificador del cliente en la sesión de Oracle	CLIENTIDENTIFIER
	Nombre del usuario externo	EXT_NAME
	Nombre del usuario que inicia sesión en el sistema operativo	OS_USER
	Nombre de la máquina o host del cliente	OS_HOST
	Identificador de la terminal del usuario	TERMINAL
	Privilegio del sistema operativo (Sysdba o SysOper). Si no se usa el privilegio se completa con NONE	OS_PRIVILEGE
¿Cuándo?	Tiempo de la creación de la entrada del registro de evento de auditoria	EXTENDED_TIMESTAMP
¿Qué?	N/A	N/A
¿Cómo?	Número de identificación para cada sesión de Oracle	SESSIONID
	Número de identificación para cada sentencia que se ejecuta	STATEMENTID
	Número de identificación para cada entrada al registro de evento de auditoria en la sesión	ENTRYID
	Identificador del proceso del sistema operativo del proceso de Oracle	OS_PROCESS
	Dueño del objeto	OBJECT_SCHEMA
	Nombre del objeto	OBJECT_NAME
	Nombre de la política de auditoria fine-grained	POLICY_NAME

	Dueño del objeto nombrado en la columna NEW_NAME	NEW_OWNER
	Nuevo nombre del objeto o el nombre del objeto subrayado	NEW_NAME
	Nombre de la acción correspondiente al código numérico.	ACTION
	Descripción de la acción	STATEMENT_TYPE
	Identificador de la transacción en la cual el objeto es accedido o modificado	TRANSACTIONID
	Código de error de Oracle generado por la acción	RETURNCODE
	Comentarios adicionales sobre el registro de eventos	COMMENT_TEXT
	Privilegios otorgados y revocados con sentencias GRANT y REVOKE	AUTH_PRIVILEGES
	Usuario al que se otorgo el privilegio	GRANTEE
	Código numérico del privilegio si se utilizó en una acción	PRIV_USED
	Resumen de la sesión, 12 caracteres por cada acción	SES_ACTIONS
	Datos de la variable en la consulta	SQL_BIND
	Texto de SQL en la consulta	SQL_TEXT
	Nombre de la edición contenida en el objeto auditado	OBJ_EDITION_NAME
	Tipo de auditoria habilitada	AUDIT_TYPE
	Identificador de la base de datos auditada	DBID

Oracle 12 C – Registro de eventos del sistema operativo

Mecanismo para el análisis de eventos	Consulta al registro de eventos del sistema operativo (seguridad o aplicación)
Privilegios	Permiso de lectura en el registro de eventos del sistema operativo

Análisis de eventos en el registro de eventos del sistema operativo

Análisis	**Descripción**
¿Quién? ¿Cuándo? ¿Qué? ¿Cómo?	La información se guarda en eventos con el número de identificación 34 y origen de datos: Oracle.oracle. En el detalle de dicho evento se encuentran los mismos campos descriptos para la tabla DBA_AUDIT_TRAIL

Oracle 12 C – Registro de eventos en la tabla DBA_FGA_AUDIT_TRAIL

Mecanismo para el análisis de eventos	Consulta a la tabla DBA_FGA_AUDIT_TRAIL
Privilegios	Permiso de ejecucion de select a la tabla DBA_FGA_AUDIT_TRAIL

Análisis de eventos de la tabla DBA_FGA_AUDIT_TRAIL

Análisis	Descripción	Campo
¿Quién?	Usuario de la base de datos que ejecutó la consulta	DB_USER
	Usuario del sistema operativo que ejecutó la consulta	OS_USER
	Nombre de la máquina /host del cliente	USERHOST
	Identificador del cliente en cada sesión de Oracle	CLIENT_ID
	Nombre externo	EXT_NAME
	Número serial de la sesión proxy, si un usuario se ha registrado a través del mecanismo de proxy	PROXY_SESSIONID
	Identificador del usuario global, si el usuario se ha registrado como un usuario empresarial	GLOBAL_UID
¿Cuándo?	Fecha y hora de la consulta en el horario de la base de datos local	TIMESTAMP
	Tiempo en la consulta en UTC (Coordinated Universal Time)	EXTENDED_TIMESTAMP
¿Qué?	N/A	N/A
¿Cómo?	Número de identificación para cada sesión de Oracle	SESSIONID
	Dueño de la tabla o vista	OBJECT_SCHEMA
	Nombre de la tabla o vista	OBJECT_NAME
	Nombre de la política Fine-Grained Auditing	POLICY_NAME
	Texto de SQL de la consulta	SQL_TEXT
	Datos de la variable en la consulta	SQL_BIND
	Comentarios	COMMENT$TEXT
	Tipos de sentencias de la consulta	STATEMENT_TYPE
	Identificador del proceso de sistema operativo del proceso Oracle	OS_PROCESS
	Identificador de la transacción por la cual el objeto se accedió o modificó	TRANSACTIONID

	Número de identificación por cada sentencia que se ejecuta	STATEMENTID
	Número de identificación por cada entrada en el registro de eventos	ENTRYID

Oracle 12 C – Registro de eventos en la vista Unified_audit_trail

Mecanismo para el análisis de eventos	Consulta a la vista Unified_audit_trail
Privilegios	Permiso de ejecución de select en la vista Unified_audit_trail

Análisis de eventos de la vista Unified_audit_trail

Análisis	**Descripción**	**Campo**
¿Quién?	Identificador de la sesión de auditoria de la sesión proxy	PROXY_SESSIONID
	Nombre del usuario de sistema operativo para la sesión de base de datos	OS_USERNAME
	Nombre del host para la cual la sesión fue generada	USERHOST
	Identificador de la terminal del usuario	TERMINAL
	Tipo de autenticación de la sesión de usuario	AUTHENTICATION_TYPE
	Nombre del usuario de la base de datos cuyas acciones fueron auditadas	DBUSERNAME
	Nombre del usuario proxy, en caso de autenticación proxy	DBPROXY_USERNAME
	Nombre del usuario externo, en caso de red o autenticación externa	EXTERNAL_USERID
	Identificador global del usuario, para un usuario registrado como usuario empresarial	GLOBAL_USERID
	Valor de SYS_CONTEXT('USERENV','DBLINK_INFO'). Valida si la conexión fue un enlace a la base de datos	DBLINK_INFO
	Nombre del usuario Real	XS_USER_NAME

	Application Security	
	Identificador de la sesión Real Application Security	XS_SESSIONID
	Identificador del cliente en cada sesión de Oracle	CLIENT_IDENTIFIER
	Roles otorgados o revocados o configurador por el comando GRANT/REVOKE/SET ROLE	ROLE
	Usuario que ejecutó la sentencia GRANT/REVOKE/AUDIT/NOAUDIT	TARGET_USER
	Usuario que fue excluído cuando se ejecutó AUDIT/NOAUDIT	EXCLUDED_USER
	Nombre del proxy user Real Application Security	XS_PROXY_USER_NAME
	El rol que esta habilitado	XS_ENABLED_ROLE
	Cookie de sesión Real Application Security	XS_COOKIE
	Nombre de la sesión namespace de Real Application Security	XS_NS_NAME
	Nombre del usuario que fue modificado en Database Vault	DV_GRANTEE
	Nombre del usuario cuya autorización OLS fue modificada	OLS_GRANTEE
	Máximo nivel de lectura asignado al usuario	OLS_MAX_READ_LABEL
	Máximo nivel de escritura asignado al usuario	OLS_MAX_WRITE_LABEL
	Mínimo nivel de escritura asignado al usuario	OLS_MIN_WRITE_LABEL
	Privilegios OLS asignados para el usuario o procedimiento almacenado confiado	OLS_PRIVILEGES_GRANTED
¿Cuándo?	Tiempo de creación de la entrada del registro de auditoria en UTC	EVENT_TIMESTAMP
	Tiempo de la sesión	RMAN_SESSION_STAMP

¿Qué?	Nombre del programa usado para la sesión de base de datos	CLIENT_PROGRAM_NAME
	Identificador del contexto por cada acción	EXECUTION_ID
¿Cómo?	Número de identificación para cada sesión de Oracle	SESSIONID
	Número de instancia especificada en el parámetro file del archivo init.ora	INSTANCE_ID
	Identificador de la base de datos de la base de datos auditada	DBID
	Número de identificación para cada entrada del registro de evento en la sesión	ENTRY_ID
	Número de identificación de cada sentencia que se ejecuta	STATEMENT_ID
	Nombre de la acción ejecutada por el usuario	ACTION_NAME
	Código de error de Oracle generado por la acción	RETURN_CODE
	Identificador del proceso del sistema operativo del proceso de la base de datos Oracle	OS_PROCESS
	Identificador de la transacción en la cual el objeto fue modificado	TRANSACTION_ID
	Nombre del esquema del objeto afectado por la acción	OBJECT_SCHEMA
	Nombre del objeto afectado por la acción	OBJECT_NAME
	SQL asociado con el evento	SQL_TEXT
	Lista de variables, si alguna esta asociada con SQL_TEXT	SQL_BINDS
	Lista separadas por comas sobre el detalle del contexto de la aplicación	APPLICATION_CONTEXTS
	El esquema del objeto nombrado en la columna NEW_NAME	NEW_SCHEMA
	Nombre del objeto después de RENAME	NEW_NAME

	Nombre de la edición contenida en el objeto auditado	OBJECT_EDITION
	Lista separada por comas de los privilegios de sistema usados para la ejecución de la acción	SYSTEM_PRIVILEGE_USED
	Privilegio de sistema otorgado/revocado por la sentencia GRANT/REVOKE	SYSTEM_PRIVILEGE
	Comando SQL AUDIT/NOAUDIT SQL	AUDIT_OPTION
	Privilegios de objeto otorgado/revocado por la sentencia GRANT/REVOKE	OBJECT_PRIVILEGES
	Muestra el esquema de objetos excluidos	EXCLUDED_SCHEMA
	Muestra los objetos excluidos desde la acción	EXCLUDED_OBJECT
	Texto comentado sobre la entrada del registro de eventos de auditoria	ADDITIONAL_INFO
	Listado de las políticas de auditoria que causan los registros de auditoria actuales.	UNIFIED_AUDIT_POLICIES
	El nombre de la política Fine-grained auditing (FGA)	FGA_POLICY_NAME
	Tiempo límite de inactividad de la sesión Real Application Security	XS_INACTIVITY_TIMEOUT
	Tipo de la entidad Real Application Security.	XS_ENTITY_TYPE
	Nombre de las operaciones en Real Application Security.	XS_TARGET_PRINCIPAL_NAME
	Nombre de la política de seguridad habilitada o inhabilitada de Real Application Security	XS_DATASEC_POLICY_NAME
	Nombre del esquema habilitado, política de seguridad de datos inhabilitada y operación global de retorno	XS_SCHEMA_NAME
	Tipo de evento callback Real Application Security	XS_CALLBACK_EVENT_TYPE

	Nombre de paquete global de callback de Real Application Security	XS_PACKAGE_NAME
	Nombre de procedimiento global de callback de Real Application Security	XS_PROCEDURE_NAME
	Nombre del atributo del namespace de Real Application Security	XS_NS_ATTRIBUTE
	El valor antiguo del atributo namespace sesion del Real Application Security	XS_NS_ATTRIBUTE_OLD_VAL
	El valor nuevo del atributo namespace sesion del Real Application Security	XS_NS_ATTRIBUTE_NEW_VAL
	Código del número de una acción para Database Vault	DV_ACTION_CODE
	Nombre de la acción correspondiente al código que aparece en la columna DV_ACTION_CODE	DV_ACTION_NAME
	Código númerico de la acción para la administración de Database Vault	DV_EXTENDED_ACTION_CODE
	Código de error en Database Vault	DV_RETURN_CODE
	El nombre único del objeto modificado de Database Vault	DV_ACTION_OBJECT_NAME
	Nombre único de la regla que fue ejecutada y causo que se dispare un evento de auditoria	DV_RULE_SET_NAME
	Comentario del texto de la entrada del evento de auditoria. Brinda mayor información sobre la sentencia auditada	DV_COMMENT
	Un documento XML que contien todos los factores identificadores para la sesión corriente	DV_FACTOR_CONTEXT
	Indica que un objeto particular de Database Vault se habilita o inhabilita	DV_OBJECT_STATUS
	Nombre de la política de Oracle Label Security (OLS) por la cual el registro de	OLS_POLICY_NAME

	auditoria se genera	
	Nombre del procedimiento almacenado de confianza cuya autorización fue modificada o fue ejecutada	OLS_PROGRAM_UNIT_NAME
	Privilegios OLS usados por un evento	OLS_PRIVILEGES_USED
	Cadenas de caracteres que representa el nivel OLS	OLS_STRING_LABEL
	Tipo del nivel del componente OLS	OLS_LABEL_COMPONENT_TYPE
	Nombre del nivel del componente OLS	OLS_LABEL_COMPONENT_NAME
	Nombre del padre del grupo OLS	OLS_PARENT_GROUP_NAME
	Valor anterior para eventos OLS ALTER	OLS_OLD_VALUE
	Nuevo valor para eventos OLS ALTER	OLS_NEW_VALUE
	Identificador de sesión RMAN	RMAN_SESSION_RECID
	La operación RMAN ejecutada por el job.	RMAN_OPERATION
	Tipo de objetos involucrados para el backup o recuperación o comandos de cambio/eliminación/crosscheck.	RMAN_OBJECT_TYPE
	Dispositivo involucrador en el RMAN job	RMAN_DEVICE_TYPE
	Parámetros durante una operación Data Pump que tengan un valor de texto.	DP_TEXT_PARAMETERS1
	Parámetro durante una operación Data Pump que tenga un valor booleano	DP_BOOLEAN_PARAMETERS1
	Muestra el número de columnas que fueron levantadas usando el método SQL*Loader	DIRECT_PATH_NUM_COLUMNS_LOADED

Análisis	Descripción	Campo
¿Quién?	Identificador de la sesión de auditoria de la sesión proxy	PROXY_SESSIONID
	Nombre del usuario de sistema operativo para la sesión de base de datos	OS_USERNAME
	Nombre del host para la cual la sesión fue generada	USERHOST
	Identificador de la terminal del usuario	TERMINAL
	Tipo de autenticación de la sesión de usuario	AUTHENTICATION_TYPE
	Nombre del usuario de la base de datos cuyas acciones fueron auditadas	DBUSERNAME
	Nombre del usuario proxy, en caso de autenticación proxy	DBPROXY_USERNAME
	Nombre del usuario externo, en caso de red o autenticación externa	EXTERNAL_USERID
	Identificador global del usuario, para un usuario registrado como usuario empresarial	GLOBAL_USERID
	Valor de SYS_CONTEXT('USERENV','DBLINK_INFO'). Valida si la conexión fue un enlace a la base de datos	DBLINK_INFO
	Nombre del usuario Real Application Security	XS_USER_NAME
	Identificador de la sesión Real Application Security	XS_SESSIONID
	Identificador del cliente en cada sesión de Oracle	CLIENT_IDENTIFIER
	Roles otorgados o revocados o configurador por el comando GRANT/REVOKE/SET ROLE	ROLE
	Usuario que ejecutó la sentencia GRANT/REVOKE/AUDIT/NOAUDIT	TARGET_USER
	Usuario que fue excluído cuando se ejecutó AUDIT/NOAUDIT	EXCLUDED_USER
	Nombre del proxy user Real Application Security	XS_PROXY_USER_NAME
	El rol que esta habilitado	XS_ENABLED_ROLE
	Cookie de sesión Real Application Security	XS_COOKIE
	Nombre de la sesión namespace de Real Application Security	XS_NS_NAME

	Nombre del usuario que fue modificado en Database Vault	DV_GRANTEE
	Nombre del usuario cuya autorización OLS fue modificada	OLS_GRANTEE
	Máximo nivel de lectura asignado al usuario	OLS_MAX_READ_LABEL
	Máximo nivel de escritura asignado al usuario	OLS_MAX_WRITE_LABEL
	Mínimo nivel de escritura asignado al usuario	OLS_MIN_WRITE_LABEL
	Privilegios OLS asignados para el usuario o procedimiento almacenado confiado	OLS_PRIVILEGES_GRANTED
¿Cuándo?	Tiempo de creación de la entrada del registro de auditoria en UTC	EVENT_TIMESTAMP
	Tiempo de la sesión	RMAN_SESSION_STAMP
¿Qué?	Nombre del programa usado para la sesión de base de datos	CLIENT_PROGRAM_NAME
	Identificador del contexto por cada acción	EXECUTION_ID
¿Cómo?	Número de identificación para cada sesión de Oracle	SESSIONID
	Número de instancia especificada en el parámetro file del archivo init.ora	INSTANCE_ID
	Identificador de la base de datos de la base de datos auditada	DBID
	Número de identificación para cada entrada del registro de evento en la sesión	ENTRY_ID
	Número de identificación de cada sentencia que se ejecuta	STATEMENT_ID
	Nombre de la acción ejecutada por el usuario	ACTION_NAME
	Código de error de Oracle generado por la acción	RETURN_CODE
	Identificador del proceso del sistema operativo del proceso de la base de datos Oracle	OS_PROCESS
	Identificador de la transacción en la cual el objeto fue modificado	TRANSACTION_ID
	Nombre del esquema del objeto afectado por la acción	OBJECT_SCHEMA
	Nombre del objeto afectado por la acción	OBJECT_NAME

	SQL asociado con el evento	SQL_TEXT
	Lista de variables, si alguna esta asociada con SQL_TEXT	SQL_BINDS
	Lista separadas por comas sobre el detalle del contexto de la aplicación	APPLICATION_CONTEXTS
	El esquema del objeto nombrado en la columna NEW_NAME	NEW_SCHEMA
	Nombre del objeto después de RENAME	NEW_NAME
	Nombre de la edición contenida en el objeto auditado	OBJECT_EDITION
	Lista separada por comas de los privilegios de sistema usados para la ejecución de la acción	SYSTEM_PRIVILEGE_USED
	Privilegio de sistema otorgado/revocado por la sentencia GRANT/REVOKE	SYSTEM_PRIVILEGE
	Comando SQL AUDIT/NOAUDIT SQL	AUDIT_OPTION
	Privilegios de objeto otorgado/revocado por la sentencia GRANT/REVOKE	OBJECT_PRIVILEGES
	Muestra el esquema de objetos excluidos	EXCLUDED_SCHEMA
	Muestra los objetos excluidos desde la acción	EXCLUDED_OBJECT
	Texto comentado sobre la entrada del registro de eventos de auditoria	ADDITIONAL_INFO
	Listado de las políticas de auditoria que causan los registros de auditoria actuales.	UNIFIED_AUDIT_POLICIES
	El nombre de la política Fine-grained auditing (FGA)	FGA_POLICY_NAME
	Tiempo límite de inactividad de la sesión Real Application Security	XS_INACTIVITY_TIMEOUT
	Tipo de la entidad Real Application Security.	XS_ENTITY_TYPE
	Nombre de las operaciones en Real Application Security.	XS_TARGET_PRINCIPAL_NAME
	Nombre de la política de seguridad habilitada o inhabilitada de Real Application Security	XS_DATASEC_POLICY_NAME
	Nombre del esquema habilitado, política de seguridad de datos inhabilitada y operación global de retorno	XS_SCHEMA_NAME

	Tipo de evento callback Real Application Security	XS_CALLBACK_EVENT_TYPE
	Nombre de paquete global de callback de Real Application Security	XS_PACKAGE_NAME
	Nombre de procedimiento global de callback de Real Application Security	XS_PROCEDURE_NAME
	Nombre del atributo del namespace de Real Application Security	XS_NS_ATTRIBUTE
	El valor antiguo del atributo namespace sesion del Real Application Security	XS_NS_ATTRIBUTE_OLD_VAL
	El valor nuevo del atributo namespace sesion del Real Application Security	XS_NS_ATTRIBUTE_NEW_VAL
	Código del número de una acción para Database Vault	DV_ACTION_CODE
	Nombre de la acción correspondiente al código que aparece en la columna DV_ACTION_CODE	DV_ACTION_NAME
	Código númerico de la acción para la administración de Database Vault	DV_EXTENDED_ACTION_CODE
	Código de error en Database Vault	DV_RETURN_CODE
	El nombre único del objeto modificado de Database Vault	DV_ACTION_OBJECT_NAME
	Nombre único de la regla que fue ejecutada y causo que se dispare un evento de auditoria	DV_RULE_SET_NAME
	Comentario del texto de la entrada del evento de auditoria. Brinda mayor información sobre la sentencia auditada	DV_COMMENT
	Un documento XML que contien todos los factores identificadores para la sesión corriente	DV_FACTOR_CONTEXT
	Indica que un objeto particular de Database Vault se habilita o inhabilita	DV_OBJECT_STATUS
	Nombre de la política de Oracle Label Security (OLS) por la cual el registro de auditoria se genera	OLS_POLICY_NAME
	Nombre del procedimiento almacenado de confianza cuya autorización fue modificada o fue ejecutada	OLS_PROGRAM_UNIT_NAME

	Privilegios OLS usados por un evento	OLS_PRIVILEGES_USED
	Cadenas de caracteres que representa el nivel OLS	OLS_STRING_LABEL
	Tipo del nivel del componente OLS	OLS_LABEL_COMPONENT_TYPE
	Nombre del nivel del componente OLS	OLS_LABEL_COMPONENT_NAME
	Nombre del padre del grupo OLS	OLS_PARENT_GROUP_NAME
	Valor anterior para eventos OLS ALTER	OLS_OLD_VALUE
	Nuevo valor para eventos OLS ALTER	OLS_NEW_VALUE
	Identificador de sesión RMAN	RMAN_SESSION_RECID
	La operación RMAN ejecutada por el job.	RMAN_OPERATION
	Tipo de objetos involucrados para el backup o recuperación o comandos de cambio/eliminación/crosscheck.	RMAN_OBJECT_TYPE
	Dispositivo involucrador en el RMAN job	RMAN_DEVICE_TYPE
	Parámetros durante una operación Data Pump que tengan un valor de texto.	DP_TEXT_PARAMETERS1
	Parámetro durante una operación Data Pump que tenga un valor booleano	DP_BOOLEAN_PARAMETERS1
	Muestra el número de columnas que fueron levantadas usando el método SQL*Loader	DIRECT_PATH_NUM_COLUMNS_LOADED

Anexo XVIII: Ejemplo de registro de evento correspondiente a inicio de sesión

Ejemplo relacionado con la pegunta Quién

Sistemas de gestión de base de datos relacional	Repositorio de eventos	Quién?	
TERADATA 13.10	DBQLogTbl	UserID	0000F805
		AcctString	$M1$
		ExpandAcctString	$M1$
		LogicalHostID	1
		LogonSource	(TCP/IP) 0a5b 10.2.49.235 10.0.5.16 5552 TOM_SO QUERYMAN 01 LSS
		ClientID	TOM_SO
		ClientAddr	10.2.49.235
		ProfileID	?
		UserName	TOM
		ProxyUser	?
		ProxyRole	?
SAP ASE 16.0 SP01	Tabla syaudits	loginname	TOM
		suid	987
SQL SERVER 12	Archivo de extensión trc	ClientProcessID	8968
		DBUserName	TOM
		Host Name	SERVIDOR_BD
		LoginName	DOMINIO DE RED\TOM_SO
		LoginSid	0X0105000000000005150 00000FEF840FA2A51D37 FA31FB0086E040000
		NT Domain Name	DOMINIO DE RED
		NT User Name	TOM_SO
		RoleName	S / D
		TargetLoginName	S/D

		TargetLoginSid	S/D
		TargetUserName	S/D
ORACLE 11 G R2	Archivos de formato XML	PROXY_SESSIONID	S/D
		GLOBAL_UID	S/D
		DB_USER	TOM
		CLIENTIDENTIFIER	S/D
		EXT_NAME	S/D
		OS_USER	TOM_SO
		OS_HOST	DOMINIO DE RED\PC
		TERMINAL	PC
		OS_PRIVILEGE	S/D

Ejemplo relacionado con la pegunta Cuándo

Sistemas de gestión de base de datos relacional	**Repositorio de eventos**	**Cuándo?**	
TERADATA 13.10	DBQLogTbl	LogonDateTime	2015-10-07 16:00:30.85
		StartTime	2015-10-07 16:00:31.58
		FirstStepTime	2015-10-07 16:00:31.69
		FirstRespTime	2015-10-07 16:00:31.91
		LastStateChange	?
SAP ASE 16.0 SP01	Tabla syaudits	eventtime	Oct 4 2015 6:05:12:395 AM
SQL SERVER 12	Archivo de extensión trc	Duration	S/D
		End Time	S/D
		Start Time	2015-10-06 18:47:00.700
ORACLE 11 G R2	Archivos de formato XML	EXTENDED_TIMESTAMP	2015-09-25T09:32:10.406000

Ejemplo relacionado con la pegunta Cómo

Sistemas de gestión de base de datos relacional	Repositorio de eventos	Cómo?	
TERADATA 13.10	DBQLogTbl	AppID	QUERYMAN
SAP ASE 16.0 SP01	Tabla syaudits	extrainfo	TOM/ase (Utilizando la herramienta ASE)
SQL SERVER 12	Archivo de extensión trc	Application Name	SQLAgent - TSQL JobStep (Job 0xC1FA71C99E438D4EA084092EA4B80917 : Step 1)
ORACLE 11 G R2	Archivos de formato XML	N/A	N/A

Ejemplo relacionado con la pegunta Qué

Sistemas de gestión de base de datos relacional	Repositorio de eventos	Qué?	
TERADATA 13.10	DBQLogTbl	NumSteps	0
		NumStepswPar	0
		MaxStepsInPar	0
		NumResultRows	0
		TotalIOCount	0
		UtilityByteCount	?
		UtilityRowCount	?
		StatementType	Help
		QueryText	HELP SESSION
		StatementGroup	Other SysOther
		QueryID	163824042890566000
SAP ASE 16.0 SP01	Tabla syaudits	event	45
		eventmod	1
		spid	410
		sequence	1
		dbid	1
		objid	NULL
		xactid	NULL

		dbname	master
		objname	NULL
		objowner	NULL
		Nodeid	1
		extrainfo	sa_role sso_role sybase_ts_role mon_role; ; ; ; , 10.0.5.16; ; TOM/ase;
SQL SERVER 12	Archivo de extensión trc	EventClass	Audit Login
		EventSubClass	S/D
		Object ID	S/D
		ObjectName	S/D
		ObjectType	S/D
		Permissions	S/D
		SPID	72
		State	S/D
		Success	1
		TextData	S/D
		Transaction ID	S/D
ORACLE 11 G R2	Archivos de formato XML	SESSIONID	1
		STATEMENTID	1
		ENTRYID	1
		OS_PROCESS	4244:3408
		OBJECT_SCHEMA	S/D
		OBJECT_NAME	S/D
		POLICY_NAME	S/D
		NEW_OWNER	S/D
		NEW_NAME	S/D
		ACTION	100
		STATEMENT_TYPE	S/D
		TRANSACTIONID	0000000000000000
		RETURNCODE	0
		COMMENT_TEXT	Authenticated by: DATABASE; Client address: (ADDRESS=(PROTOCOL=tcp)(HOST=10.0.1.78)(PORT=4927))
		AUTH_PRIVILEGES	S/D
		GRANTEE	S/D
		PRIV_USED	5
		SES_ACTIONS	S/D
		SQL_BIND	S/D
		SQL_TEXT	S/D
		OBJ_EDITION_NAME	S/D
		DBID	274847654
		AUDIT_TYPE	1

Bibliografía

[1] National Institute of Standards and Technology (NIST), Special Publication 800- 92 Guide to Computer Security Log Management, Technology Administration U.S. Department of Commerce, Gaithersburg, 2006.

[2] ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission), Information technology — Security techniques — Code of practice for information security controls, ISO copyright, Geneve, 2013

[3] Database Administration TD 13.10, http://www.info.teradata.com/templates/eSrchResults.cfm?prodline=&txtpid=&txtrelno=&txtttlkywrd=DBADMIN,DBADMIN&rdsort=Title&srtord=Asc&nm=Database+Administration
(consultada el 13/7/2016)

[4] SAP Adaptive Server Enterprise 16.0 SP01 Document Version: 1.1 – 2015-12-11 Security Administration Guide, http://www.help.sap.com/Download/Multimedia/zip-ase1601/SAP_ASE_Security_Administration_Guide_en.pdf.
(consultada el 13/8/2015)

[5] 10775A - Administering Microsoft® SQL Server® 2012 Databases, https://skillpipe.courseware-marketplace.com/reader/es-ES/Account/Login?ReturnUrl=%2Freader%2F
(Consultada el 1/9/2014. Sitio de acceso restringido)

[6] Oracle Corporation, Oracle Database 11g: Security Student Guide, Oracle University, Estados Unidos de Norteamérica. 2007.

[7] Oracle Database 12c: "Auditoría Unificada (Unified Auditing)", http://www.oracle.com/technetwork/es/articles/idm/auditoria-unificada-database-12c-2538967-esa.html
(consultada el 24/8/2015)

[8] Oracle Database 11g:The Top Features for DBAs and Developers, http://www.oracle.com/technetwork/articles/sql/11g-security-100258.html
(consultada el 2/10/2014)

[9] Database SQL Language Reference AUDIT,

http://docs.oracle.com/cd/E11882_01/server.112/e26088/statements_4007.htm
(consultada el 3/10/2014)
[10] Database Security Guide Introduction to Auditing,
http://docs.oracle.com/database/121/DBSEG/auditing.htm#DBSEG1023
(consultada el 29/8/2015)
[11] sp_audit_write (Transact-SQL) SQL Server 2012,
https://technet.microsoft.com/en-us/library/gg471540(v=sql.110).aspx
(consultada el 7/9/2015)
[12] Understanding a sample SQL audit event,
https://www.ultimatewindowssecurity.com/sqlserver/auditlog/sampleevent.aspx
(consultada el 28/9/2015)
[13] Database Reference DBA_AUDIT_STATEMENT,
http://docs.oracle.com/cd/B19306_01/server.102/b14237/statviews_3055.htm#i1619442
(consultada el 28/9/2015)
[14] Database Reference DBA_AUDIT_SESSION,
http://docs.oracle.com/cd/B19306_01/server.102/b14237/statviews_3054.htm
(consultada el 28/9/2015)
[15] Database Reference DBA_AUDIT_OBJECT,
https://docs.oracle.com/cd/B19306_01/server.102/b14237/statviews_3051.htm#i1618972
(consultada el 28/9/2015)
[16] Database Reference DBA_AUDIT_EXISTS,
http://docs.oracle.com/cd/B28359_01/server.111/b28320/statviews_3067.htm
(consultada el 28/9/2015)
[17] Database Reference V$XML_AUDIT_TRAIL,
http://docs.oracle.com/cd/E11882_01/server.112/e40402/dynviews_3128.htm
(consultada el 30/9/2015)
[18] TEMA 8:EL CIERRE DEL PROYECTO,
https://www.arquitectes.cat/ca/system/files/tema8.pdf
(consultada el 22/01/2016)

[19] Tracking Query Behavior with Database Query Logging: Operational DBAs
https://www.info.teradata.com/doclist.cfm?RetainParams=Y&FilterCall=Y&selDocType=101
(consultada el 12/10/17)
[20] Version Update - 16.0 SP03 PL02
https://help.sap.com/viewer/791c41982ee345a19c4ec4b774222c4f/16.0.3.2/en-US/86a9ea4e98fe40ef83b893933af3def1.html
(consultada el 10/11/17)
[21] SQL Server Audit (Database Engine)
https://docs.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-database-engine
(consultada el 13/10/17)
[22] Oracle Database 12c Enterprise Edition—Features
https://www.oracle.com/database/enterprise-edition/features.html
(consultada el 13/11/17)
[23] SecureSphere Database Audit an Protection
https://imperva.com/products/data-security/database-audit-protection
(consultada el 13/1/18)