Plan de Auditoría para Bases de Datos Multitenant en Oracle

César Augusto Zapata Urrea[1]

Resumen

La auditoría a bases de datos es un método que busca recopilar información para analizarla, examinarla y evaluarla de tal forma que de un juicio y proporcione los mecanismos necesarios para valorar bases de datos en la nube utilizando controles y técnicas que identifican, mitigan y eliminan riesgos.

Este trabajo presenta una breve descripción de que son bases de datos Oracle Multitenant incluidas las definiciones de container y pluggables, así como tres estándares posibles para implementar auditorías en este tipo de configuración, dando detalles técnicos, posibles controles y evaluando la mejor opción para buscar el aseguramiento de datos.

[1] CESAR AUGUSTO ZAPATA URREA. Ingeniero de Sistemas egresado de la Universidad Distrital Francisco José de Caldas. Especialista en Administración de Empresas de la universidad del Rosario. Estudiante Especialización en auditoria de sistemas universidad Antonio Nariño. Plan de auditoría para bases de datos multitenant.

e-mail: czapata69@uan.edu.co

El lector tendrá a su disposición una propuesta de implementación de auditoria para identificar a que nivel puede ser implementada logrando con ello minimizar vulnerabilidades de acuerdo a la opción elegida conociendo porque Audit Vault es la elegida y como su uso facilita el trabajo de la auditoría de sistemas en bases de datos multitenant.

Palabras claves: multitenant, container, pluggables

Abstract

Database auditing is a method that seeks to collect information to analyze, examine and evaluate it in such a way that it makes a judgment and provides the necessary mechanisms to value databases in the cloud using controls and techniques that identify, mitigate and eliminate risks.

This work presents a brief description of what Oracle Multitenant databases are, including container and pluggable definitions, as well as three possible standards to implement audits in this type of configuration, giving technical details, possible controls and evaluating the best option to search for the data assurance.

The reader will have at his disposal an audit implementation proposal to identify at what level it can be implemented, thereby minimizing vulnerabilities according to the option chosen, knowing why Audit Vault is the chosen one and how its use facilitates the work of systems auditing. in multitenant databases.

Keywords: multitenant, container, pluggables

Introducción

Contar con una solución en la nube que proporcione disponibilidad y costos razonables hace que las bases de datos que comparten recursos de cómputo, software y administración, sean una alternativa viable para compañías de cualquier tamaño. Las bases de datos multitenant en general y la solución de Oracle en particular, son de interés por su acceso y fácil gestión, por lo cual esta investigación tiene relevancia al poner de presente las alternativas disponibles de auditoria presentando distintas opciones de implementación.

Debido a que el acceso a la información de auditoría debe ser configurada, puede ser restringida, por lo cual en la tecnología multitenant no ha sido implementada masivamente a pesar de sus bondades, razón por la cual una vez que se adquieren soluciones de este tipo se debe involucrar un profesional de bases de datos y otro de auditoria de sistemas para que la implementación sea más eficiente y certera con la coordinación del área de TI.

En bases de datos no multitenant se utiliza auditoria enfocada únicamente en los componentes individuales de la base de datos, pero en una arquitectura multitenant es conveniente ampliar el alcance de la auditoria para que cubra los nuevos elementos que la componen. Situaciones como esta dejan entrever las vulnerabilidades y posibles riesgos creados por usuarios que tienen acceso a la información de cualquier base de datos del container.

En documentos de expertos (Ona Systems) se puede identifican vulnerabilidades a diferentes niveles como por ejemplo privilegios excesivos, abuso de los privilegios dados, aumento de privilegios no autorizados, vulnerabilidades de la plataforma, inyección de SQL, auditoría débil, vulnerabilidades en los protocolos de las bases de datos y autenticación débil.

Al implementar una auditoria enfocada en bases de datos Multitenant es pertinente tener en cuenta aspectos adicionales a una gestión en bases de datos tradicionales toda vez que las particularidades de esta tecnología presuponen un conocimiento no solo en auditoria sino también en el ambiente propio de dicha solución integrando metodologías ya utilizadas para proporcionar los controles necesarios que propendan por bases de datos confiables, seguras, singulares y especialmente con un nivel de trazabilidad idóneo dando un valor agregado a la manera tradicional como se ha venido realizando en las bases de datos tradicionales, por lo tanto este documento pretende darle respuesta a la pregunta, ¿Cuáles son las alternativas en la auditaría de sistemas a bases de datos multitenant, para evaluar la integridad, confiabilidad y disponibilidad de la información en la computación en la nube?

De esta manera el impacto sobre la estabilidad, confiabilidad y oportunidad de los datos sensibles de una empresa es grande al generar las sinergias necesarias para crear un ambiente eficiente y seguro.

Objetivo general

Realizar un plan de auditoria para bases de datos Multitenant en Oracle que minimice las vulnerabilidades asociadas al procesamiento de datos.

Objetivo específicos

a. Describir la configuración y funcionamiento de las bases de datos Multitenant en Oracle.

b. Identificar metodologías de auditoria que sean apropiadas para un sistema de bases de datos Multitenant en Oracle.

c. Diseñar un plan de auditoria para un sistema de base de datos Multitenant en Oracle.

Metodología

Para la elaboración de este artículo se utilizará la metodología deductiva hasta llegar a un plan específicos de auditoria utilizando un tipo de estudio descriptivo explicativo que permita llegar a los objetivos mediante la recolección de información sobre el funcionamiento y configuración de auditorías de sistemas de bases de datos multitenant en Oracle.

Como fuentes de información se utiliza la revisión documental, consulta a la base de conocimiento de Oracle Support, consultas en bases de datos electrónicas como ProQuest, IEEE, conferencias en foros especializados, revistas, videos y en general cualquier material en la web que haga referencia al tema de auditoria en bases de datos multitenant.

Marco Contextual

En Colombia normalmente se utilizan las normas ISO (Organización Internacional para la Estandarización) y la Comisión Electrotécnica Internacional (IEC) que: *se encargan de establecer estándares y guías relacionados con sistemas de gestión y aplicables a cualquier tipo de organización internacionales y mundiales, con el propósito de facilitar el comercio, facilitar el intercambio de información y contribuir a la transferencia de tecnologías.* (auditoria-informat.blogspot.com, 2016), especialmente la familia de normas ISO/IEC 27000 que dan estándares de seguridad y son muy útiles al momento de hacer una auditoria de sistemas.

En el presente artículo hará referencia a las tres opciones más relevantes de auditoria de bases de datos en Oracle: Oracle Audit Vault, Oracle Unified Auditing, Oracle Standard Auditing que pueden

suplir las necesidades de información de un auditor de TI (Tecnología de la Información). Como lo menciona Poddar y Nadgi (2010) en su artículo "*Desarrollar y desplegar las Soluciones Multitenant brindadas por la Web utilizando el Middleware de IBM*" o Yenugula y Ayapán (2015) en su artículo "*Replicación de múltiples bases de datos "Pluggable" (PDBs) en una arquitectura "Multitenant" utilizando Oracle GoldenGate 12c*", existen diferentes alternativas para implementar una solución multitenant. A partir de esta consideración, este trabajo se enfocará en tres alternativas de implementación de auditoría para bases de datos multitenant Oracle, entendiendo por *Multitenant* (termino que se acuño en la década de 1960), como: *una configuración orientada a soluciones en la nube que utiliza hardware y software de alto desempeño para formalizar recursos, minimizar costos y compartir la administración, cuando las empresas alquilaban tiempo en grandes máquinas de computo (mainframes) que eran raros y de costo alto, en aquel entonces se llamaba tiempo compartido y varios clientes podían acceder a las mismas aplicaciones al mismo tiempo lo cual solo era posible en estos los grandes servidores*. (Damation by QuinStreet Inc.)

Una configuración típica de esta arquitectura se puede ver en la figura 1. Arquitectura Multitenant Oracle 12c – Consolidación de recursos y bases de datos:

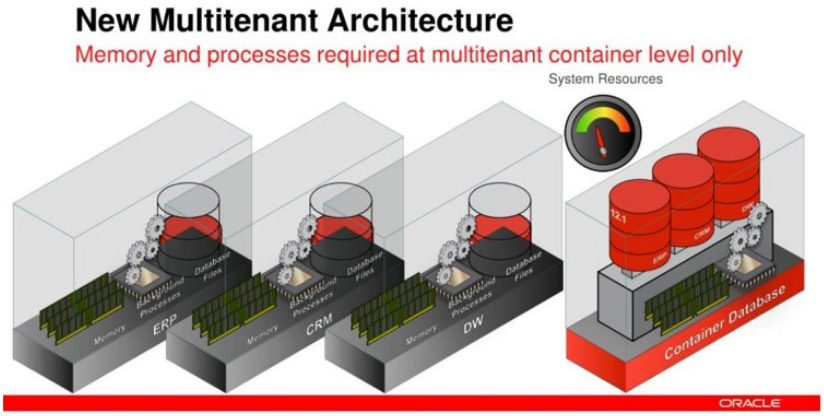

Figura 1. Arquitectura Multitenant Oracle 12c – Consolidación de recursos y bases de datos
Fuente: *Oracle Corporation*

Con esta tecnología la información del negocio se almacena dentro de estructuras particulares conocidas como *Pluggables Databases (PDBs*), las cuales se pueden asimilar conceptualmente a las bases individuales iniciales (ERP – CRM – DW), que están física y lógicamente definidas dentro del CDB[2]donde se ubican los metadatos comunes a todas las PDBs creadas gestionando sus recursos individualmente y compartiendo recursos, actividades, seguridad y usuarios que les son comunes.

Como se observa en la figura 2 pluggables database, las PDB en una configuración multitenant son fácilmente conectadas (ingresadas en el CDB) y desconectadas (eliminadas del CDB) gracias a la gestión compartida de recursos y la individualización de componentes, esta característica es conocida como Container el cual se define como la estructura creada para soportar bases de datos Multitenant almacenando el diccionario de datos raíz y la relación de las pluggables entre sí con el CDB.

Figura 2. Pluggables database
Fuente: Oracle Corporation

[2] CDB: Container Database

Resultados

La *arquitectura multitenant* es una configuración de software orientada a la nube especialmente para SaaS:*" El software como un servicio (SaaS) es un modelo, en el cual un proveedor en la nube desarrolla y mantiene un software de aplicaciones y proporciona actualizaciones automáticas a los clientes a través de internet mediante el pago por uso." (Que es software as a Service (SaaS) Oracle Colombia, 2014)*, que se caracteriza por utilizar uno o más servidores para alojar una instancia única (conjunto de memoria y servicios de base de datos) para compartir recursos físicos como CPU y disco, como se puede observar en la figura 3, Container database, que muestra PDB fuera del container y como se integran una vez se ha configurado el CDB.

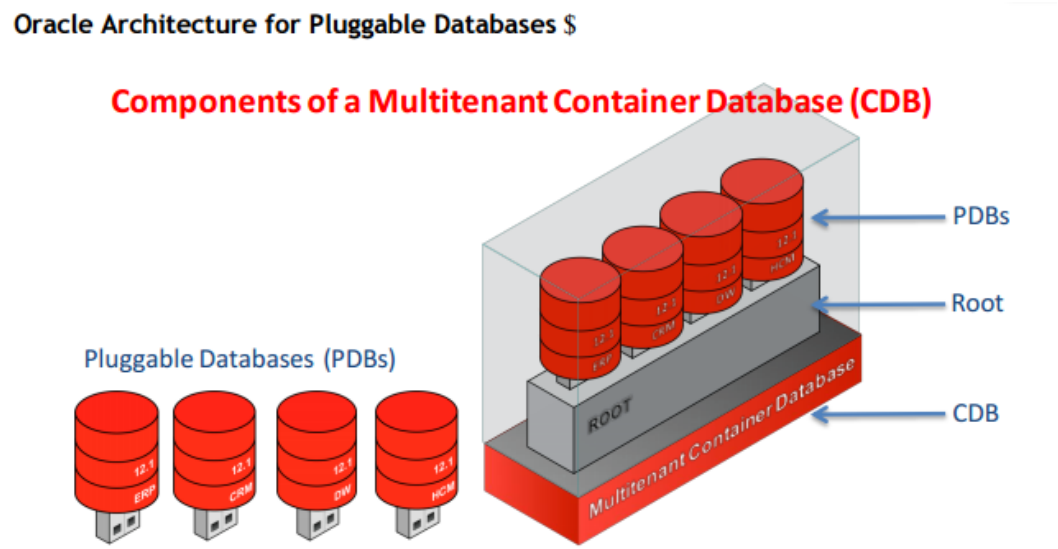

Figura 3, Container database
Fuente: Oracle Corporation

Implementar una solución de auditoría en configuraciones multitenant implica conocer sus principales componentes. En la figura 4, Arquitectura Container Oracle 12c, se observa una configuración típica de CDB con sus componentes de memoria (S.G.A.), CDB (Datafiles, Control files, Redo Log files) y PDB (Application 1, SALES, HR)

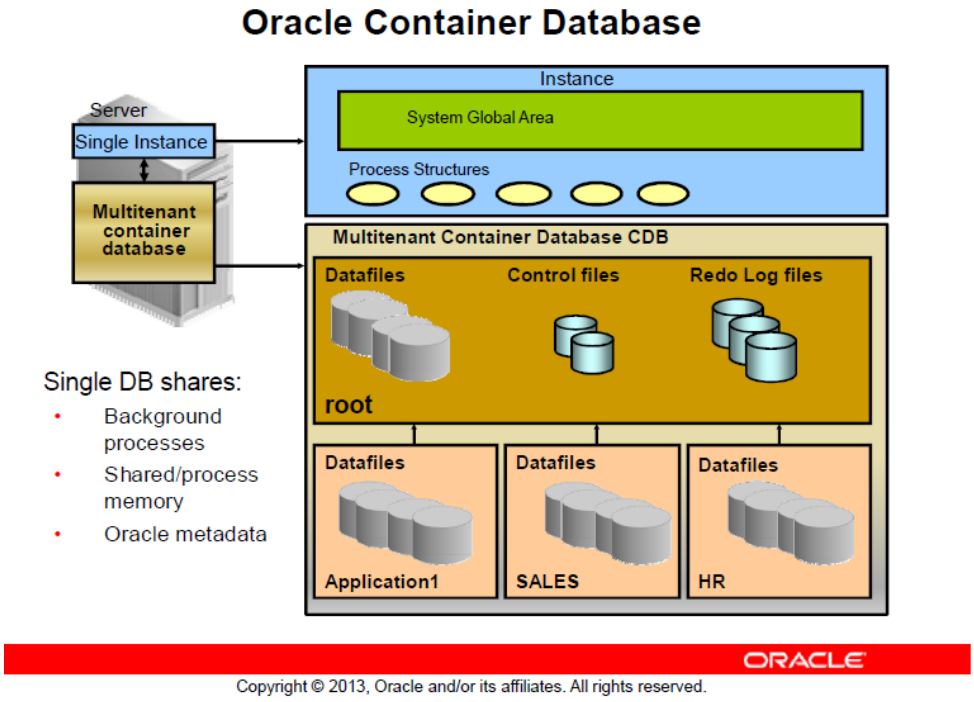

Figura 4. Arquitectura Container Oracle 12c
Fuente: Oracle Corporation 13 de enero de 2014

Cada uno de estos elementos puede ser utilizado por los diferentes usuarios de las bases de datos de acuerdos a los privilegios y roles asignados. Es por ello que una buena política de auditoría debe considerarlos, tanto en su ubicación física (en el CDB o En la PDB), como en las actividades que sobre ellos se pueden realizar a través de los usuarios.

Es por esto que conocer a que nivel se definen los usuarios, como se observan en la figura 5, permite caracterizarlos para crear políticas de auditoria enfocadas al CDB, a la PDB o a ambas.

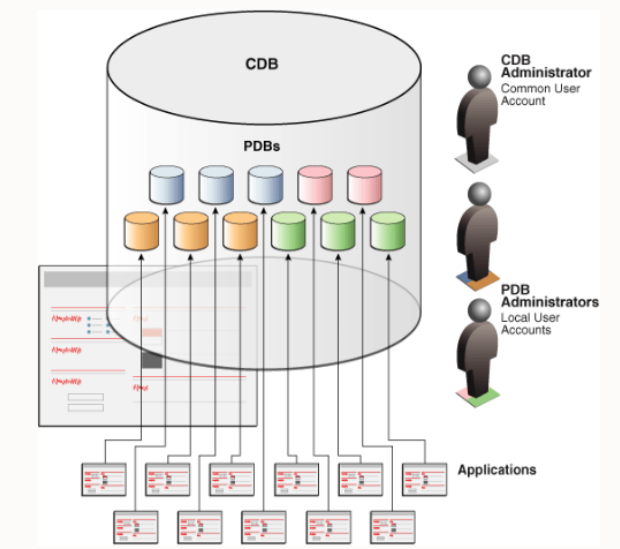

Figura 5. Container database y usuarios.
Fuente: https://docs.oracle.com/

Usuario común (common user account): es un usuario que se define a nivel de CDB y tiene el mismo nombre de usuario y credenciales de autenticación en todos los PDB con privilegios para conectarse en cualquiera de ellos y realizar operaciones administrativas.

Usuario local (local user account): un usuario local es un usuario de la base de datos que existe solo en un PDB y tiene privilegios administrativos solo en ese PDB.

Metodologías de auditoria apropiadas para un sistema de bases de datos Multitenant en Oracle.

Cada día es más relevante la gestión de auditoria que se puede y debe hacer en las empresas en áreas de cumplimiento, privacidad y seguridad que estén asociadas a regulaciones como Sarbanes-Oxley que estableció normas específicas para endurecer los controles en las empresas, particularmente en lo relacionado con la obligación de certificar los estados financieros y sus procesos de elaboración y la evaluación de los controles internos. (René M. Castro V., 2004)

Oracle Audit Vault

> Permite configuración, análisis y recopilación de información convirtiendo los datos en recurso de seguridad para dar cumplimiento y seguridad a regulaciones que gobiernos de todo el mundo han promulgado asociadas a controles financieros, de asistencia médica y privacidad. (Oracle Corporation, 2007).

Es claro que cada regulación tiene sus propias características y requerimientos, por ejemplo, la ley Sarbanes-Oxley (SOX) requiere que los ejecutivos certifiquen la precisión de los estados financieros. La ley Healthcare Insurance Portability and Accountability Act (HIPAA) requiere la protección de la información sensible relacionada con el área de asistencia médica, la ley Payment Card Industry Data Security Act (PCI) exige que los ejecutivos monitoreen el acceso a los datos personales de los propietarios de tarjetas de crédito. Debido a ello al pensar en implementar una auditoria se debe considerar las regulaciones de privacidad y cumplimiento junto con las políticas y procedimientos de seguridad adecuados ya que la información generada debe ser analizada y organizada para poder ser útil en la auditoria.

Según Computer Crime Research Center (Center, 2005) que en su estudio de Seguridad y Delitos Informáticos CSI/FBI 2005, más del 70% de los ataques y las pérdidas de datos es perpetrado por personas internas a la empresa, con altos niveles de autorización de acceso, es por ello que la auditoria a sistemas multitenant que tienen usuarios con estas características son una buena elección para utilizar Oracle Audit Vault, ya que recopila los datos de auditoría desde distintas fuentes: la base de datos Oracle o cualquier otra, el sistema operativo, los registros de transacciones (log y trace) entre otros y resuelve estos problemas de seguridad y auditoría consolidando la información de esas fuentes, haciendo detección de cambios de datos asociados con usuarios regulares y privilegiados, protegiendo los datos de auditoría de modificaciones y alteraciones, como lo describe Oracle en su documento Guía del administrador de Oracle® Audit Vault (Oracle Corporation 2013, s.f.), se prestan servicios de auditoria con modelos prediseñados y gestión de información fácil de utilizar de tal manera que

implementar una auditoria a bases de datos multitenant es sencilla porque una vez realizada la configuración de la herramienta provee: almacén de datos de auditoría, consola de administración, informes prediseñados, alertas tempranas como se ve en la figura 6: Tablero de alertas, modelos de auditoría preconfigurados, auditoría de recopilación de datos y gestión de almacenamiento entre otros.

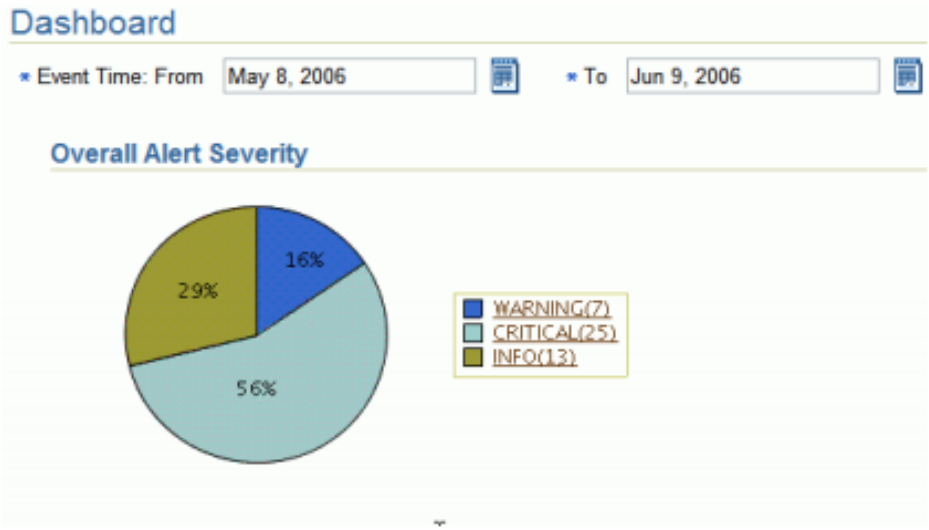

Figura 6. Tablero de alertas Audit Vault
Fuente: Oracle Corporation

De manera complementaria en el documento Oracle® Audit Vault and Database Firewall Auditor's Guide (Oracle Corporation, 2020) especifica como un auditor puede utilizar este producto para configurar auditoria a bases de datos en general y multitenant en particular, definiendo políticas de auditoría, alerta, usuarios, reportes, accesos y fuentes de información entre otros componentes. En la figura 7, configuración de Oracle Audit Vault, se pueden observar un esquema de funcionamiento típico.

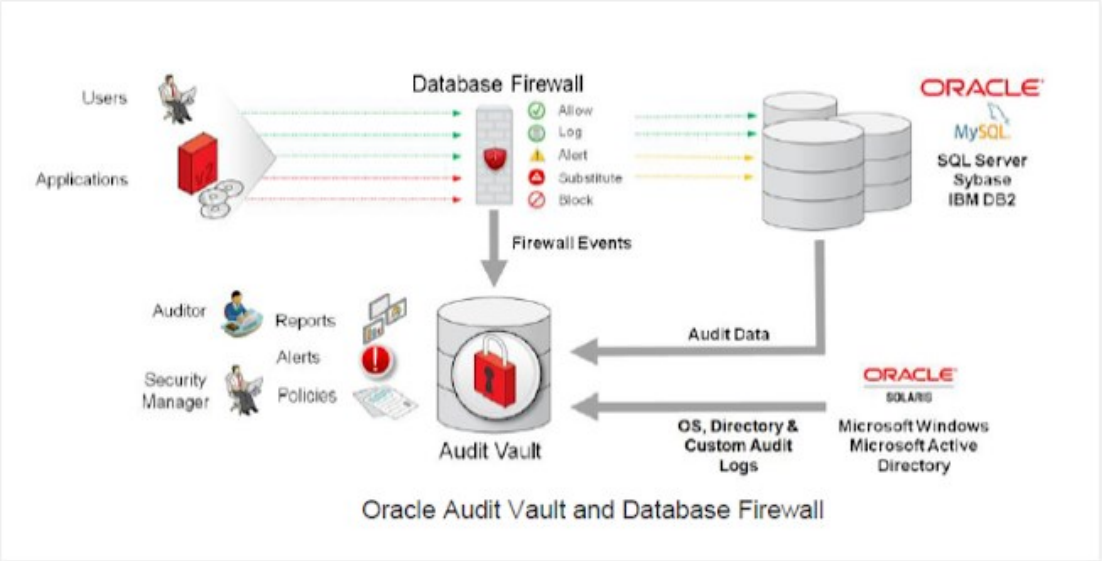

Figura 8. Configuración de Oracle Audit Vault
Fuente: Oracle Corporation

Oracle Unified Auditing

Otra alternativa para auditar una base de datos Multitenant es la auditoria unificada de Oracle que se basa en la tecnología Fine Grained Auditing (FGA por sus siglas en inglés o auditoria de grano fino) que posibilita la creación de políticas de auditoría personalizadas y orientadas a los objetos y eventos de interés.

Su implementación debe ser realizada por un ingeniero de TI con conocimientos específicos en el área de auditoria de bases de datos y FGA, es una buena práctica que la configuración realizada permita integrarla con Oracle Audit Vault para hacer más robusta la auditoria al permitir generar alertas automáticas de acuerdo a definiciones previamente establecidas.

Al tener una auditoria unificada en bases de datos multitenant se debe fundamentalmente seguir los siguientes pasos: Habilitar la auditoria FGA, definir las políticas de aplicación (que incluyen el ámbito, frecuencia, condiciones de aplicación y registro de evento) y finalmente crear reportes de consulta de acuerdo a las necesidades del auditor.

> Accessing a table between 9 p.m. and 6 a.m. or on Saturday and Sunday
> Using an IP address from outside the corporate network
> Selecting or updating a table column
> Modifying a value in a table column

Figura 9. Fine-Grained Auditing
Fuente: www. https://blog.yannickjaquier.com/

De esta manera se busca minimizar el alto número de registros que normalmente se generan en diferentes fuentes enfocándose en los puntos de interés como se puede ver en la *figura 10. Oracle Unified Auditing*, donde se observa cómo se gestionan los repositorios de datos.

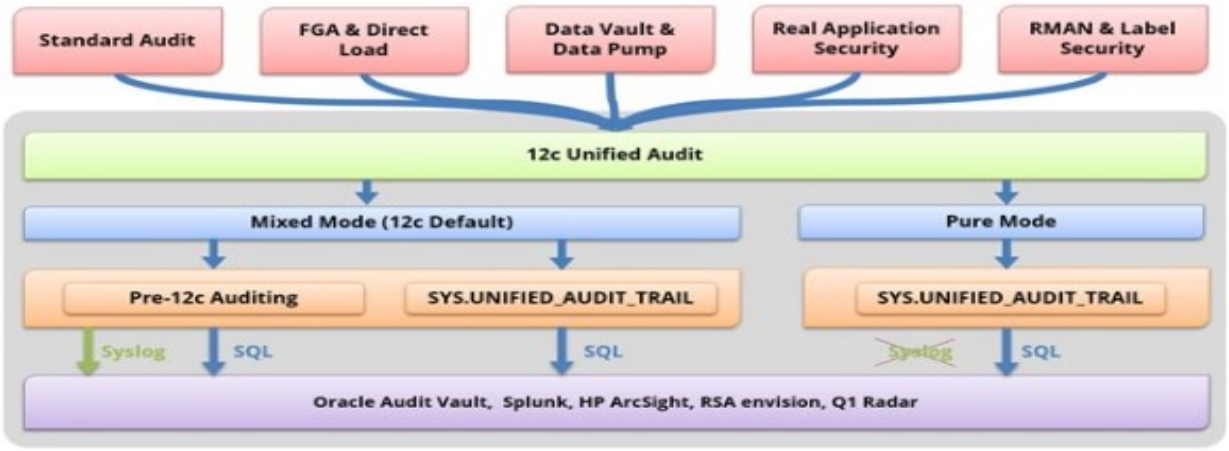

Figura 10. Oracle Unified Auditing
Fuente: GeodaMaster by Yannick Jaquier

De esta manera en un ambiente multitenant se puede establecer el ámbito al cual la auditoria se va a definir creando políticas basadas en los privilegios o roles del sistema u objeto de interés, siendo posible crear dichas políticas a nivel de CDB para todo el CDB o en un nivel PDB para un solo PDB.

Si se define a nivel de container las políticas se pueden utilizar en los PDB, lo que permite tener estándares de auditoría como se observa en la Figura 11. Niveles de autoría: CDB UNIFIED AUDIT TRAIL

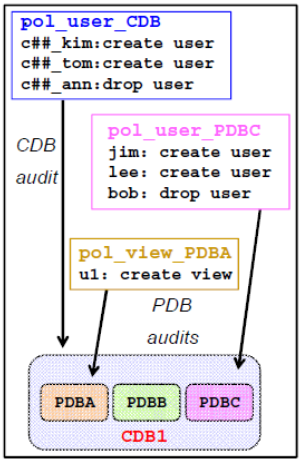

Figura 11. Niveles de autoría: CDB UNIFIED AUDIT TRAIL
Fuente: Oracle 12c Multitenant Arquitecture

Una vez la información está en los repositorios (tablas de auditoria), un profesional de TI debe realizar los script o programas necesarios para que esta información pueda ser verificada por el auditor de sistemas. Para esto se generan reportes en diferentes formatos o se implementan aplicaciones propias con este propósito, o se realizan interfaces con aplicaciones de auditoria tipo Oracle Audit Vault para que sea la fuente de la información.

Oracle Standard Auditing

La auditoría Estándar de Oracle es la forma más antigua de hacer seguimiento a actividades que se consideren sospechosas dentro de un CDB o PDB. Está disponible desde las primeras versiones de Oracle y por tanto su alcance ha evolucionado con el motor. Sin embargo, requiere un conocimiento especial sobre los parámetros que se deben utilizar para que sea eficiente y productiva, llegando a tener una mayor complejidad en comparación a otras opciones debido a que la interrelación existente entre dichos parámetros y los eventos que se desean auditar hacen que la experiencia del profesional de TI en estos procesos juegue un papel de gran relevancia.

Este tipo de auditoria produce información sobre la operación que se auditó, el usuario que realizó la operación y la fecha y hora de la operación. Los registros de auditoría se pueden almacenar en la pista de auditoría

de la base de datos o en archivos del sistema operativo e incluye el registro de operaciones sobre privilegios, esquemas, objetos y declaraciones.

Su característica principal es que los datos se generan sin valor agregado y un profesional de TI debe crear los reportes que permitan consultarla. La Figura 12. Auditoria Standard muestra donde se pueden ubicar los registros de auditoría.

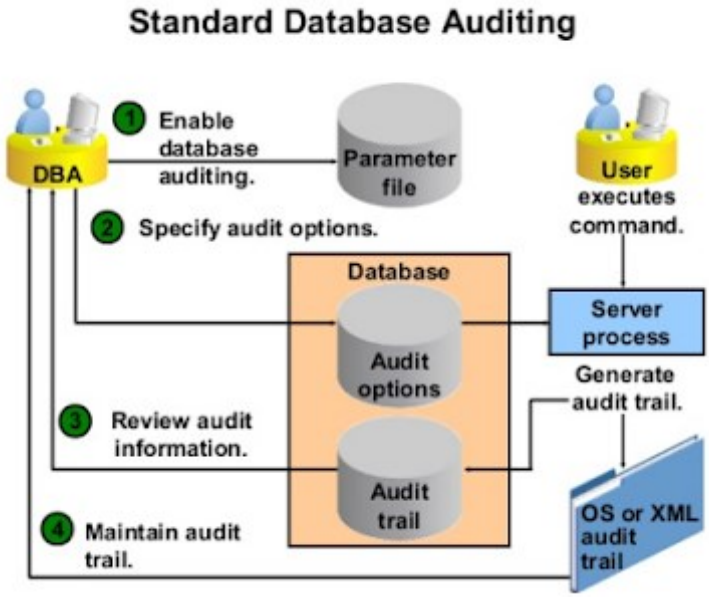

Figura 12. Auditoria Standard
Fuente: Oracle 12c Multitenant Arquitecture

En este tipo de auditoria se debe definir más conceptos para activar el registro, tales como: objeto, nivel, destino, clase de registro. Si se define erróneamente genera gran cantidad de información que puede consumir el espacio del disco generando problemas en toda la base de datos.

Existen metodologías que permiten facilitar la labor del auditor y se han presentado tres opciones viables para obtener la información relevante para poder realizar un informe de auditoría en bases de datos multitenant.

Sin embargo, la implementación normalmente está basada en la experiencia del auditor y por tanto dependen de él; por ello a continuación se presenta una tabla de comparación de las opciones

presentadas como se puede ver en la tabla 1 Criterios de Evaluación y en la tabla 2 Matriz de comparación metodologías de auditoria en Oracle Multitenant.

Tabla 1 Criterios de Evaluación

Valor	Descripción
1	no significativo
2	bajo
3	medio
4	medio - alto
5	alto

Fuente: elaboración propia

Tabla 2 Matriz de comparación metodologías de auditoria en Oracle Multitenant

ITEM	Oracle Audit Vault	Oracle Unified Auditing	Oracle Standard Auditing
Costo (1 alto - 5 bajo)			
Hardware	2	4	3
Software	3	2	5
Alcance			
Incluye leyes Internacionales	5	3	2
Incluye leyes Nacionales	5	3	2
Incluye normativas empresariales	3	2	2
Se adapata a nuevos requerimientos	4	3	2
Bajo conocimiento tecnico para implementar la auditor	4	3	2
Detalle en registro de Auditoria			
Datos especificos par usuarios del container	3	4	3
Datos especificos par usuarios del pluggable	3	4	4
Datos de diferentes fuentes	4	1	1
Configurable el detalle de colección de información	3	5	2
Generación de Reportes de Auditoria			
Graficas disponibles	5	3	2
Tendencias de eventos disponibles	4	2	2
Seguimiento de alertas disponibles	4	2	2
Satisfacción de requerimientos particulares - personalización			
Plantillas predefinidas	4	2	2
Fácil personalización	4	2	2
PUNTAJE TOTAL	60	45	38
VALORACION PROMEDIO	3,8	2,8	2,4

Fuente: elaboración propia

Plan de auditoria para un sistema de base de datos Multitenant en Oracle.

De acuerdo con el estudio de cada una de estas metodologías se considera que la mejor alternativa es Audit Vault porque protege los entornos de base de datos en forma transparente, se adapta fácilmente a los cambios de seguridad en el CDB y el las PDB, facilitando la generación de

reportes dinámicos y flexibles sobre seguridad a diferentes niveles ya que contiene una amplia gama predefinida de ellos. Los detalles técnicos se encuentran en el manual Audit Vault and Database Firewall Administrator's Guide (Oracle Corporation, 2015).

Como consecuencia de lo anterior y teniendo presente que una propuesta de implementación de auditoria en bases de datos multitenant debe considerar el nivel al que se van a definir las políticas y el ámbito de la auditoría es lo que va a determinar los límites de la misma, es fundamental definir el alcance. A continuación, se presenta un plan de auditoría a bases de datos multitenant que muestra que actividades de configuración se deben realizar en Audit Vault para que genere la información de auditoria requerida. El plan tiene las siguientes fases que se pueden ver en la Tabla 3 plan de auditoria:

Observación: permite conocer el ambiente de CDB y los productos de software Oracle instalados, el diseño y estructura de bases de datos.

Seguridad: Identificar las características desde el sistema operativo que restringen el acceso al software de base de datos, a sus archivos de almacenamiento, configuración y que los usuarios tienen los privilegios apropiados.

Configurar Auditoria: Configurar la auditoría de la base de datos de acuerdo a los requerimientos de negocios.

Reportes: Generación de reportes básico para una auditoría en bases de datos multitenant Oracle, para lo cual se utiliza la interfaz gráfica propia de Audit Vault.

Tabla 3 Plan de auditoría

ENTENDIMIENTO		
ITEM	**DESCRIPCION**	**ACTIVIDAD**
1	Versiones Oracle	Identificar productos y versiones de Oracle
2	Modelo de datos.	Identificar modelos de datos lógicos a auditar
3	Modelos lógicos	Identificar modelos lógicos que a auditar
4	Archivo de configuración	Obtener copia de archivo init.ora
5	Diccionario de datos	Obtener principales vista
6	Obtener archivo INIT.ORA	Verificar parametros definidos
7	Parámetros definidos por PDB	Obtener lista de parámetros con SHOW PARAMETERS
8	Parámetros definidos por CDB	Obtener lista de parámetros con SHOW PARAMETERS
9	Perfiles de usuario en S.O.	Revisar los perfiles de usuario del S.O. sobre ORACLE_HOME, ORACLE_BASE, ORACLE_GRID para determinar si solo usuarios autorizados
10	Usuarios del CDB	Identificar los usuarios definidos a nivel de CDB
11	Usuarios del PDB	Identificar los usuarios definidos a nivel de PDB
12	Verificar privilegios de usuario	Determine si los privilegios de acceso asignados a cada usuario son
13	Gestion de password usuarios PDB	Determine si los passwords son regularmente cambiados para todos los usuarios, incluyendo OPS$ usernames
14	Gestion de password usuarios default PDB	Determine si los passwords por default asociados con los usernames SYS y SYSTEM se cambiaron después de su instalación.
15	Identificar tablas a auditar	Con ALL_OBJECTS identificar que tablas son de interes para auditar
16	Niveles de acceso sobre objetos	Identificar el nivel de acceso concedido a los objetos a través de las vistas DBA_TAB_GRANTS del diccionario de Datos
17	Identificar permisos en cascada de usuarios en el CDB	Verificar uso de WITH GRANT OPTION en los usuarios
18	Control de usuarios	Verificar usuarios con privilegios con select CON_ID, GRANTEE, PRIVILEGE, COMMON from cdb_sys_privs where GRANTEE='C##_USU1' order by PRIVILEGE;
19	Habilitar auditoría	Ir INIT.ORA y colocar el parametro AUDIT_TRAIL está colocada en TRUE
20	Definir nivel de auditoria	Configurar el parametro AUDIT_TRAIL de acuerdo al detalle de auditoria requerido(none-os-db-db, extended)
21	Conectarse a la PDB de interes o al Configurar Auditoría	connect sys@PDB2 as sysdba o connect / as sysdba A nivel de CDB o de PDB realizar las siguientes actividades
22	Definir detalle de políticas de auditoría	Audit options: Systemwide or object-specific or role – Optional WHEN condition EVALUATE PER STATEMENT – CONTAINER = CURRENT | ALL
23	Activar registro de auditoría	AUDIT and NOAUDIT
24	Definir usuarios a auditar	ALL, es el default (C##_ usuario de CDB - usuario PDB, sin prefijo)
25	Crear políticas de auditoria - conección	Connect to the root or the specific PDB CONNECT / AS SYSDBA CONNECT system@PDBC
26	Crear políticas de auditoria - definición para privilegios del sistema, acciones y roles	CREATE AUDIT POLICY audit_mixed_pol1_CDB PRIVILEGES DROP ANY TABLE ACTIONS CREATE TABLE, DROP TABLE, TRUNCATE TABLE ROLES emp_role;
27	Crear políticas de auditoria - definicion para objetos especificos	CREATE AUDIT POLICY audit_objpriv_pol2_PDB ACTIONS EXECUTE, GRANT ON hr.raise_salary_proc;
28	Crear políticas de auditoria - restricciones	CREATE AUDIT POLICY audit_mixed_pol3_PDB ROLES hr_role WHEN 'SYS_CONTEXT (''USERENV'', ''SESSION_USER'')=''JIM''' EVALUATE PER SESSION
29	Habilitar politicas de auditoría - TODOS los usuarios	AUDIT POLICY audit_mixed_pol1_CDB;
30	Habilitar politicas de auditoría - ALGUNOS de los usuarios	SQL> CONNECT system@PDBC SQL> AUDIT POLICY audit_objpriv_pol2_PDB BY scott, oe;
31	Habilitar auditoría por eventos	SQL> AUDIT POLICY audit_syspriv_pol1 WHENEVER SUCCESSFUL;
32	Revisar Registros de auditoria	SELECT con_id, ACTION_NAME FROM CDB_UNIFIED_AUDIT_TRAIL;

Fuente: Elaboración propia

La interfaz de Reportes Oracle Audit Vault se puede observar en la Figura 13, que provee informes predefinidos entre los cuales se encuentran los siguientes: acceso predeterminados, acceso a datos por usuarios, ejecuciones de procedimientos, sesiones de usuario, alertas entre otros.

- Descripción de la "Figura 3-1 Página de informes predeterminados"

Figura 13. Interfaz de Reportes Oracle Audit Vault
Fuente: Oracle 12c Multitenant Arquitecture

Conclusiones

Oracle 12c consolida el uso de múltiples instancias de bases de datos dentro de una estructura centralizada conocida como container y de esta manera optimiza el uso de recursos de hardware y software.

Las bases de datos multitenant se configuran de acuerdo a las necesidades del cliente con una o más PDB que son independientes en los datos que gestionan, en los usuarios locales que utilizan y en los

registros de auditoria que generan, pero comparten usuarios con las demás PDB llamados usuarios comunes que pueden realizar operaciones sobre cualquier base de datos.

Existen tres principales opciones para configurar auditoría a bases de datos multitenant, donde su implementación debe contar con la participación de profesionales de TI y de auditoria para obtener la configuración adecuada para registrar e interpretar adecuadamente la información de obtenida.

Las alternativas en la auditaría de sistemas a bases de datos multitenant, para evaluar la integridad, confiabilidad y disponibilidad de la información en la computación en la nube deben considerar criterios financieros, de alcance, conocimientos técnicos y requerimientos particulares. En este trabajo se identifica que la mejor opción es utilizar Audit Vault como herramienta para configurar la auditoria.

El plan de auditoría presentado responde a los elementos de interés que se desean evaluar siendo una buena práctica auditar la actividad que tienen los usuarios comunes en el CDB, particularmente en creación, modificación y borrado de objetos a nivel de PDB.

Oracle Audit Vault brinda reportes predefinidos, análisis y consolidación de información, detecta amenazas y genera alertas con una configuración sencilla que permite al auditor generar reportes de auditoria de forma ágil, rápida y oportuna.

Referencias

Center, C. C. (2005). Obtenido de http://www.crime-research.org/legislation/

Damation by QuinStreet Inc. (s.f.). Obtenido de https://www.datamation.com/cloud-computing/what-is-multi-tenant-architecture.html

Gómez, Deiby. (2016). *Oracle Database 12.2: Application Containers.* Obtenido de https://www.oracle.com/technetwork/es/articles/database-performance/application-containers-part1-3422253-esa.html

Kumar, Y. V., Yenugula Venkata , R., & Ayapán , J. C. (2015). *https://www.oracle.com/technetwork/es/articles/database-performance/bases-de-datos-pluggable-3708769-esa.html*. Obtenido de https://www.oracle.com/technetwork/es/articles/database-performance/bases-de-datos-pluggable-3708769-esa.html

Ministerio de Hacienda y Crédito Público. (2009). Auditores, Estandares Internacionales de Auditoria, aplicación en Colombia. En M. d. Hacienda.

Ona Systems. (s.f.). *Vulneerabilidades importantes que afectan la seguridad en bases de datos.* Obtenido de https://www.onasystems.net/vulnerabilidades-importantes-afectan-la-seguridad-bases-datos-las-empresas/

Oracle Corporation. (2007). *ORACLE AUDIT VAULT Trust-but-Verify.* Obtenido de https://www.oracle.com/technetwork/es/documentation/317444-esa.pdf

Oracle Corporation. (2013). *Oracle Database 12c: Managing Multitenant Architecture.*

Oracle Corporation 2013. (s.f.). *Oracle® Audit Vault Administrator's Guide*. Obtenido de https://docs.oracle.com/cd/E11062_01/admin.1023/e11059/avadm_intro.htm

Oracle Corporation. (2015). *Audit Vault and Database Firewall Administrator's Guide.*

Oracle Corporation. (2020). *Oracle® Audit Vault and Database.*

Poddar, I., & Nadgi, D. (2010). *Desarrollar y desplegar las Soluciones Multi-Tenant brindadas por la Web utilizando el Middleware de IBM*. Obtenido de https://www.ibm.com/developerworks/ssa/library/ws-multitenantpart5/ws-multitenantpart5-pdf.pdf

Que es software as a Service (SaaS) Oracle Colombia. (2014). Obtenido de https://www.oracle.com/co/applications/what-is-saas/

René M. Castro V. (2004). REVISTA INTERNACIONAL LEGIS DE CONTABILIDAD Y AUDITORÍA N°:20. *REVISTA INTERNACIONAL LEGIS DE CONTABILIDAD Y AUDITORÍA N°:20*, 13-42.

Sanches, J. C. (2012). Los métodos de investigación. En J. C. Sanches, *Los métodos de investigación* (págs. 81-93). Madrid: Ediciones Diaz Santos.