ORACLE

Oracle Cloud Services   **Oracle Database**   **Oracle Middleware** | **Categories** |

Oracle Partner Innovation & Modernization Center

ORACLE DATABASE | Friday, February 28, 2014

Oracle Database 12c Security: New Unified Auditing

By: Tarek Salama

According to the 2012 Data Breach Investigations Report from the Verizon RISK Team, more than 1 billion database records were breached around the world from 2004 to 2011. As companies endeavor to secure sensitive data within the enterprise, the need has emerged for cost-effective, easy-to-use tools that can be quickly deployed company wide. To that end, Oracle has merged and advanced two

proven security solutions—Oracle Audit Vault and Oracle Database Firewall — into a single software appliance-based platform: Oracle Audit Vault and Database Firewall. (source:

http://www.oracle.com/technetwork/issue-archive/2013/13-mar/o23news-1906468.html)

With the introduction of Oracle Database 12c, we have a plethora of new security features, as listed in the Oracle Database 12c Security Guide, amongst which we now have a brand new Unified Audit Data Trail, enabling selective and even more effective auditing inside the Oracle database using policies and conditions. A consolidated audit data trail has many advantages, especially when it's integrated with Audit mining tools.

In previous releases of Oracle Database, there were separate audit trails for individual components:

- SYS.AUD$ for the database audit trail,

- SYS.FGA_LOG$ for fine-grained auditing,

- DVSYS.AUDIT_TRAIL$ for Oracle Database Vault, Oracle Label Security,

- and so on.

In this release, these audit trails are all unified into one, viewable from the UNIFIED_AUDIT_TRAIL data dictionary view for single-instance installations or Oracle Database Real Application Clusters environments.

On Oracle Database 12c, with Unified Auditing and Conditional Auditing, you get the ability to configure precise,

context-dependant logging which should reduce the performance overhead associated with database auditing and enable more effective analysis of audit logs.

Conditional Auditing supports highly selective logging policies that minimize log entries to specific events such as particular SQL statements including the actions CREATE or ALTER originating from outside specific application servers identified by IP address. Other variables include programs, time periods and connection types.

With Unified Auditing you can now run analysis reports on an entire set of audit data in one operation, rather than having to first gather them into one location before performing the analysis. Audit mining tools such as Oracle Audit Vault now can look at one location rather than several in order to gather audit records. A unified audit trail ensures that the audit information is consistently formatted and contains consistent fields. Database auditing in 12c can be integrated with the Oracle Audit Vault and Database Firewall, used to control and monitor SQL network activity. Unlike standard packet filter firewalls that operate at layers 3 and 4 of the OSI model, the Oracle Database Firewall performs highly accurate analysis of SQL traffic at layer 7 and can block SQL injection attacks.
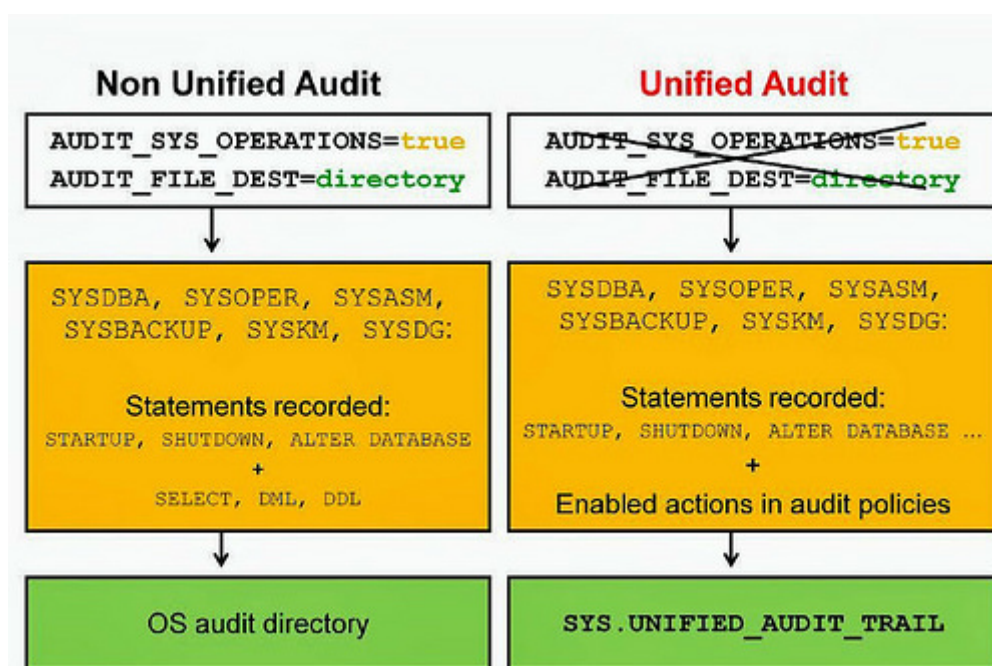
The ability to configure precise, context-dependant logging should reduce the performance overhead associated with database auditing and enable more effective analysis of audit logs. Conditional Auditing supports highly selective logging policies that minimize log entries to specific events such as particular SQL statements including the actions CREATE or ALTER originating from outside specific application servers identified by IP address. Other variables include programs, time periods and connection types. Conditional Auditing also introduces AUDIT_ADMIN and AUDIT_VIEWER roles to better protect the integrity of policies and logs which are now part of single unified architecture.

Significant Redesign in Auditing Functionality

For this release, the auditing functionality has been significantly redesigned from the functionality used in previous releases. When you install a new Release 12 Oracle database, the full sets of auditing enhancement features (unified auditing) are automatically available. If you upgrade from a previous release, then you are given the option of using some of the new audit features and the audit functionality from the release that you upgraded from. Oracle strongly recommends that you migrate to the full set of latest audit features.

New Schema for the Unified Audit Trail

As part of the unified audit trail enhancement, a new schema, AUDSYS, will be used solely for storage of the unified audit trail data table. The existing audit data in the AUD$ and FGA_LOG$ system tables, audit metadata, and audit PL/SQL packages, will continue to reside in the SYS schema.
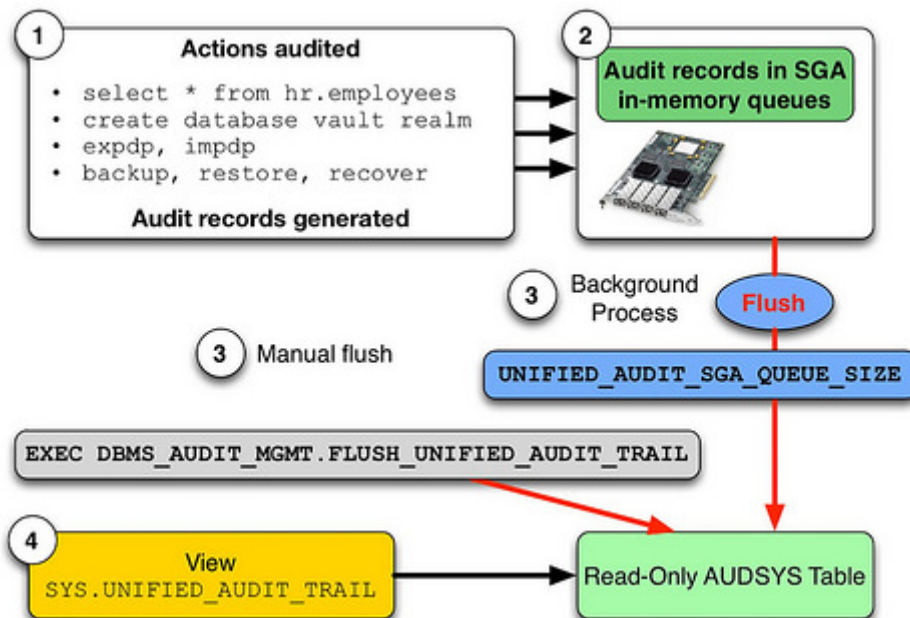
Separation of Duties for Audit Administration

For better separation of duty, two new database roles are now available for use with auditing: AUDIT_ADMIN, for audit configuration and audit trail administration, and AUDIT_VIEWER, for viewing and analyzing audit data.

Faster Audit Performance

This release provides a much faster audit performance than in previous releases of Oracle Database. You also can control how the audit records are written to the audit trail, whether immediately or queued to memory.

Auditing In 12c

- Ability to Audit Any Role.

- Auditing Application Context Values.

- Auditing Oracle Database Real Application Security Events.

- Auditing Oracle Recovery Manager Events.

- Auditing Oracle Database Vault Events.

- Auditing Oracle Label Security Events.

- Auditing Oracle Data Mining Events.

- Auditing Oracle Data Pump Events.

- Auditing Oracle SQL*Loader Direct Load Path Events.

- Moving Operating System Audit Records into the Unified Audit Trail.

Checkout the "Auditing with Unified Auditing" for further information how to audit operations of all RDBMS and other components like RMAN, Oracle Data Pump using the new 12*c* Unified Auditing feature, consolidating all audit trails into a single unified audit trail table

For your enquiries feel free to contact us at partner.imc@beehiveonline.oracle.com

ORACLE
PARTNERNETWORK
PARTNER HUB

Stay Connected

Oracle Newsletters

Join the discussion

Visit the Oracle Blog

Learn more

Contact Us

Learn more

Site Map   Legal Notices   Terms of Use   Privacy   Cookie Preferences