INTEGRIGY

WHITE PAPER

Oracle 12c
Unified Auditing

APRIL 2016

ORACLE 12C UNIFIED AUDITING

Version 1.0 – October 2014
Version 1.5 – April 2016

Authors: Michael A. Miller, CISSP, CISSP-ISSMP, CCSK and Stephen Kost

If you have any questions, comments, or suggestions regarding this document, please send them via e-mail to info@integrigy.com.

The Information contained in this document includes information derived from various third parties. While the Information contained in this document has been presented with all due care, Integrigy Corporation does not warrant or represent that the Information is free from errors or omission. The Information is made available on the understanding that Integrigy Corporation and its employees and agents shall have no liability (including liability by reason of negligence) to the users for any loss, damage, cost or expense incurred or arising by reason of any person using or relying on the information and whether caused by reason of any error, negligent act, omission or misrepresentation in the Information or otherwise. Furthermore, while the Information is considered to be true and correct at the date of publication, changes in circumstances after the time of publication may impact on the accuracy of the Information. The Information may change without notice.

Table of Contents

Oracle Release 12c Auditing

Introduction

In Oracle 12c, a new database auditing foundation has been introduced. Oracle Unified Auditing changes the fundamental auditing functionality of the database. In previous releases of Oracle, there were separate audit trails for each individual component. Unified Auditing consolidates all auditing into a single repository and view. This provides a two-fold simplification: audit data can now be found in a single location and all audit data is in a single format. Oracle 12c Unified Auditing supports –

- Standard database auditing
- SYS operations auditing (AUDIT_SYS_OPERATIONS)
- Fine Grained Audit (FGA)
- Data Pump
- Oracle RMAN
- Oracle Label Security (OLS)
- Database Vault (DV)
- Real Application Security (RAS)
- SQL*Loader Direct Load

Unified Auditing comes standard with Oracle Enterprise Edition; no additional license is required. It is installed by default, but not fully enabled by default. There are two modes of operation to allow for a transition from pre-12c auditing –

- **Mixed Mode** – default 12c option. All pre-12c log and audit functionality and configurations work as before. New Unified Auditing functionality is also available. Log data is available in both the traditional locations as well as the new view `SYS.UNIFIED_AUDIT_TRAIL`. Also, log data continues to be written in clear text when Syslog is used.
- **Full Mode or PURE mode** – enabled only by stopping the database and relinking the Oracle kernel. Once enabled, pre-12c log and audit configurations are ignored, and audit data is saved using the Oracle SecureFiles, which is a proprietary file format. Because of this, Syslog is not supported. All audit data can be found in the view `SYS.UNIFIED_AUDIT_TRAIL.`

For more information on Unified Auditing can be found here:

- 12c Unified Auditing, Oracle Database Security Guide 12*c* Release 1 (12.1)
  http://docs.oracle.com/database/121/DBSEG/auditing.htm#DBSEG1023
- Predefined Unified Audit Policies, Oracle Database Security Guide 12*c* Release 1 (12.1)
  http://docs.oracle.com/database/121/DBSEG/audit_config.htm#DBSEG356

Figure 1 – Auditing Pre-Oracle 12c

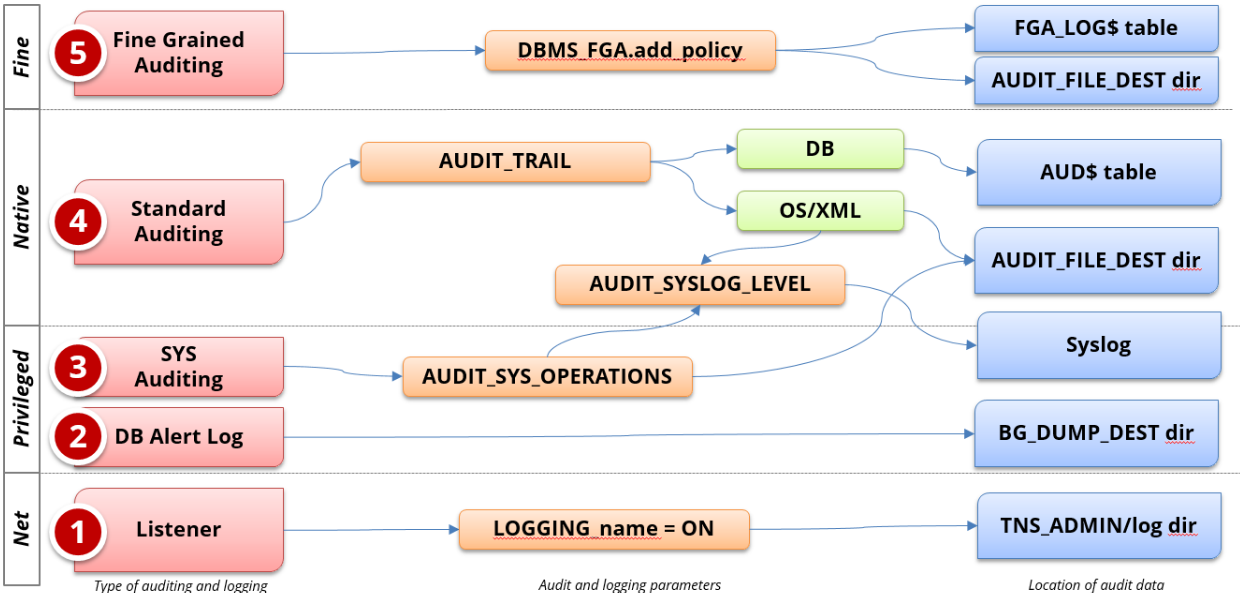


Figure 2 – Oracle 12c Unified Auditing – Mixed Mode

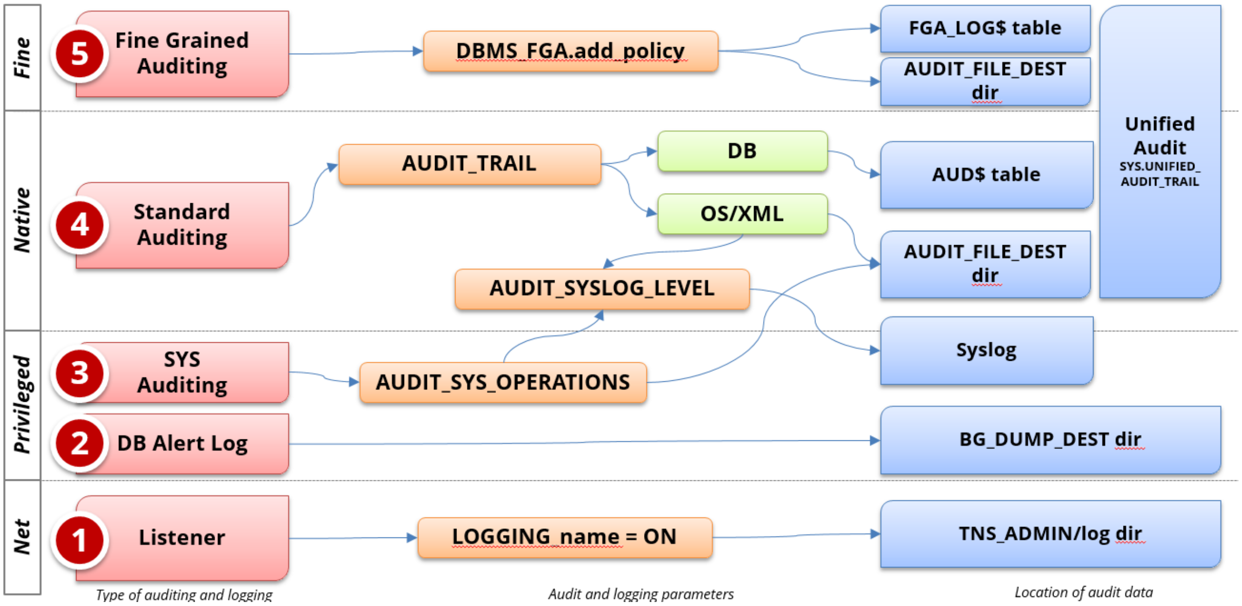


Figure 3 – Oracle 12c Unified Auditing – Pure Mode

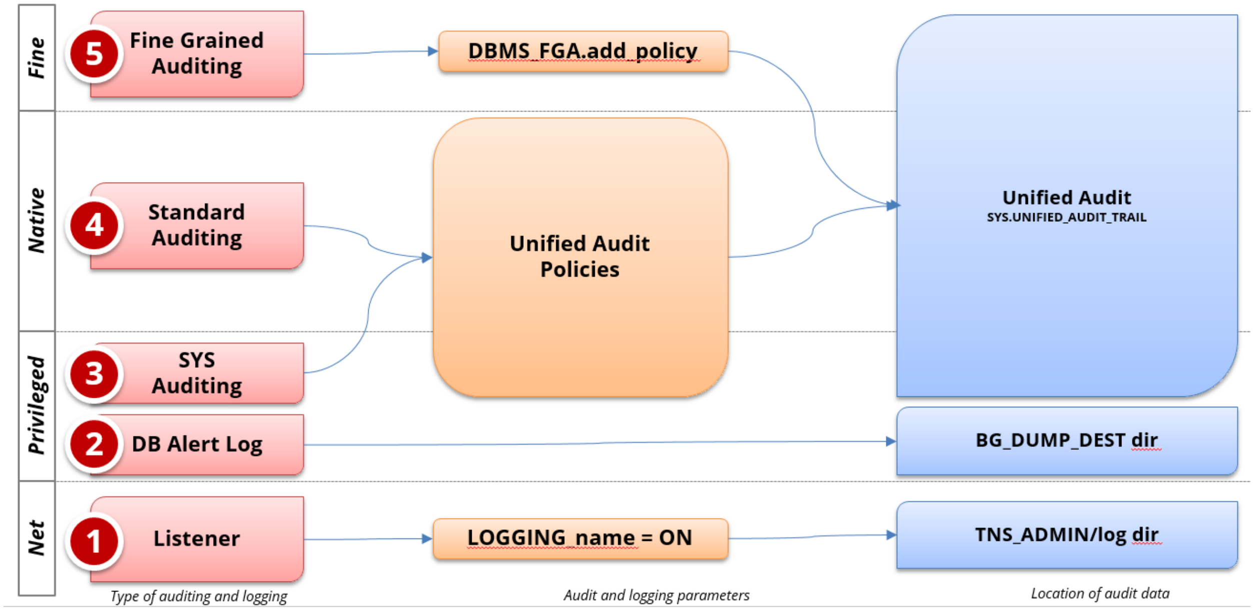
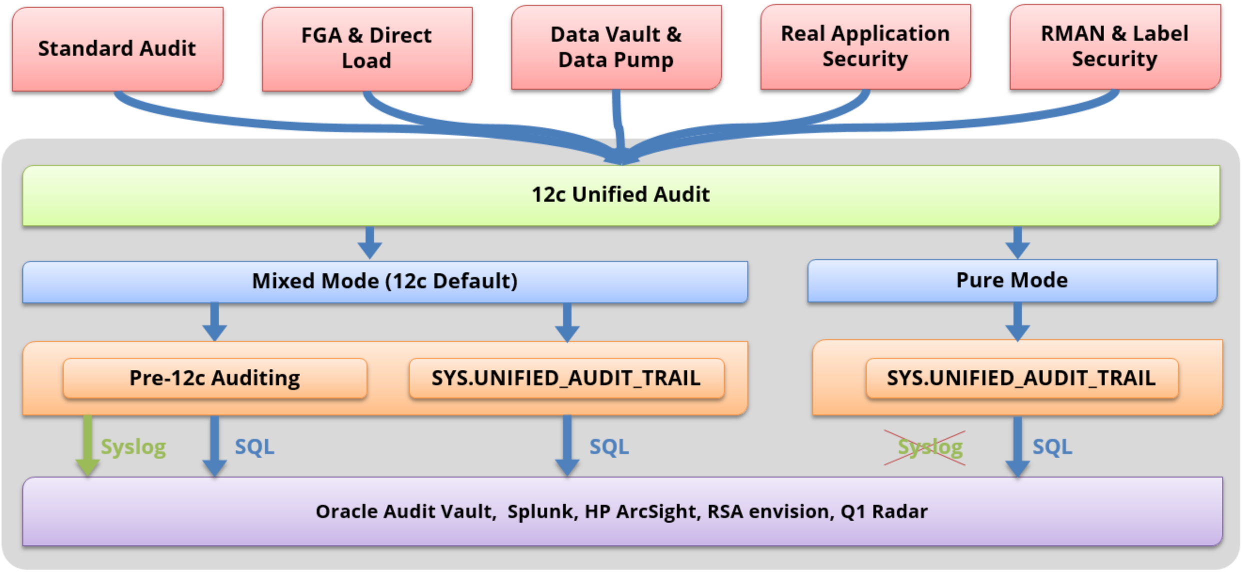


Figure 4 – Oracle 12c Unified Audit



UNIFIED AUDIT CONFIGURATION SETTINGS

How to check which mode is being used? Use the following SQL –

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

The result will be **TRUE** or **FALSE**. If **TRUE**, the database is using PURE Unified Auditing. If **FALSE,** the database is using Mixed Mode, which is the Oracle 12c default. Remember that `V$OPTION` shows what database options are installed, and `V$PARAMETER` shows the startup parameters for the options which have been installed. Unified Auditing is enabled by being installed and not by being configured in `V$PARAMETER`.

Unified Auditing is configured through policies. If Oracle 12c tenant databases (PDBs) are being used, these polices can be applied to common objects in all PDBs or to individual PDBs. The table below show the policies installed and/or enabled by default –

Unified Audit Polices Installed With Oracle 12c

Policy Name	Default Enabled	Description
ORA_SECURECONFIG	Yes	Secure configuration audit options
ORA_RAS_POLICY_MGMT	No	Oracle Real Application Security administrative actions on application users, roles, and policies.
ORA_RAS_SESSION_MGMT	No	Run-time Oracle Real Application Security session actions and namespace actions
ORA_ACCOUNT_MGMT	No	Commonly used user account and privilege settings for create user, role, and privilege grants
ORA_DATABASE_PARAMETER	No	Audits commonly used Oracle Database parameter settings e.g., initialization file (spfile) changes

To query what policies have been defined you may use –

```
        SELECT * FROM SYS.AUDIT_UNIFIED_POLICIES
```

To query what polices have been enabled you may use –

```
        SELECT * FROM SYS.AUDIT_UNIFIED_ENABLED_POLICIES
```

Pure Unified Audit

Mixed mode is intended by Oracle to introduce Unified Auditing and provide a transition from the traditional Oracle database auditing. Migrating to pure Unified Auditing requires the database be stopped, the Oracle binary linked to `uniaud_on`, and then restarted. This operation can be reversed if auditing needs to be changed back to Mixed Mode.

When changing from Mixed to pure Unified Audit, two key changes occur. The first is the audit trails are no longer written to their traditional pre-12c audit locations. Auditing is consolidated into the Unified Audit views and stored using Oracle SecureFiles. Oracle Secured Files use a proprietary format which means that Unified Audit logs cannot be viewed using editors such vi and may preclude or affect the use of third party logging solutions such as Splunk or HP ArcSight. As such, Syslog auditing is not possible with Pure Unified Audit.

Unified Audit Mixed vs. Pure Mode Audit Locations

System Tables	Mixed Mode	Pure Unified Audit Impact
SYS.AUD$	Same as 11g	Exists, but will only have pre-unified audit records
SYS.FGA_LOG$	Same as 11g	Exists, but will only have pre-unified audit records

The second change is that the traditional audit configurations are no longer used. For example, traditional auditing is largely driven by the AUDIT_TRAIL initialization parameter. With pure Unified Audit, the initialization parameter AUDIT_TRAIL is ignored.

Unified Audit Mixed vs. Pure Mode Audit Configurations		
System Parameters	**Mixed Mode**	**Pure Unified Audit Impact**
AUDIT_TRAIL	Same as 11g	Exists, but will not have any effect
AUDIT_FILE_DEST	Same as 11g	Exists, but will not have any effect
AUDIT_SYS_OPERATIONS	Same as 11g	Exists, but will not have any effect
AUDIT_SYSLOG_LEVEL	Same as 11g	Exists, but will not have any effect
UNIFIED_AUDIT_SGA_QUEUE_SIZE	Same as 11g	Yes

For more information –

- Oracle Securefile format http://www.oracle.com/technetwork/database/features/secure-files/securefiles-160920.html
- Pure vs. Mixed Unified Audit impact on audit configurations, see table G-1 http://docs.oracle.com/database/121/DBSEG/audit_changes.htm#DBSEG341
- "How To Enable The New Unified Auditing In 12c?" Note ID 1567006.1, Oracle Corporation, 23 August 2013, https://support.oracle.com/rs?type=doc&id=1567006.1

Mixed Mode

Mixed Mode is the default auditing mode for Oracle 12c. Oracle describes Mixed Mode auditing as a means of becoming familiar with Unified Auditing prior to migrating to Pure Unified Auditing. Mixed Mode allows for all traditional, pre-12c log and audit functionality to co-exist with Unified Auditing. More importantly, Mixed Mode will support any current Syslog-based logging solution.

Mixed mode auditing provides the following key capabilities –

- All existing (pre-12c) auditing initialization configurations and parameters are used such as AUDIT_TRAIL, AUDIT_FILE_DEST, AUDIT_SYS_OPERATIONS, and AUDIT_SYSLOG_LEVEL
- The format of the audit records remains the same as in Oracle Database 11*g* Release 2
- Writes mandatory audit records to the traditional audit trails

- If the AUDIT_SYS_OPERATIONS initialization parameter is set to TRUE, writes audit records only to the traditional audit trails

With Mixed Mode, audit data can be found both in the traditional locations as well as in SYS.UNIFIED_AUDIT_TRAIL. This is because the Unified Auditing Policy ORA_SECURECONFIG is enabled by default. ORA_SECURECONFIG audits the same default audit settings from Oracle Database Release 11*g.* Integrigy recommends to either periodically purge Unified Auditing data or disable the policy. To disable ORA_SECURECONFIG policy follow the instructions in Oracle Support Note Doc ID 1624051.1.

The following table shows the definition of the default policy ORA_SECURECONFIG. Note the column 'Common' that shows that the policy is defined for all PDBs (tenant) databases.

Mixed Mode Default Unified Policy ORA_SECURECONFIG			
Audit Option	**Option Type**	**Common**	**Integrigy Framework**
ADMINISTER KEY MANAGEMENT	SYSTEM PRIVILEGE	YES	E11 – Privileged commands
ALTER ANY PROCEDURE	SYSTEM PRIVILEGE	YES	E13 – Objects
ALTER ANY SQL TRANSLATION PROFILE	SYSTEM PRIVILEGE	YES	E11 – Privileged commands
ALTER ANY TABLE	SYSTEM PRIVILEGE	YES	E13 – Objects
ALTER DATABASE	SYSTEM PRIVILEGE	YES	E11 – Privileged commands
ALTER DATABASE LINK	STANDARD ACTION	YES	E13 – Objects
ALTER PLUGGABLE DATABASE	STANDARD ACTION	YES	E11 – Privileged commands
ALTER PROFILE	STANDARD ACTION	YES	E14 – Modify configuration settings
ALTER ROLE	STANDARD ACTION	YES	E8 – Modify role
ALTER SYSTEM	SYSTEM PRIVILEGE	YES	E14 – Modify configuration settings
ALTER USER	STANDARD ACTION	YES	E6 – Modify user account
AUDIT SYSTEM	SYSTEM PRIVILEGE	YES	E11 – Privileged commands
CREATE ANY JOB	SYSTEM PRIVILEGE	YES	E13 – Objects
CREATE ANY LIBRARY	SYSTEM PRIVILEGE	YES	E13 – Objects
CREATE ANY PROCEDURE	SYSTEM PRIVILEGE	YES	E13 – Objects
CREATE ANY SQL TRANSLATION PROFILE	SYSTEM PRIVILEGE	YES	E11 – Privileged commands
CREATE ANY TABLE	SYSTEM PRIVILEGE	YES	E13 – Objects
CREATE DATABASE LINK	STANDARD ACTION	YES	E13 – Objects
CREATE DIRECTORY	STANDARD ACTION	YES	E13 – Objects
CREATE EXTERNAL JOB	SYSTEM PRIVILEGE	YES	E13 – Objects
CREATE PLUGGABLE DATABASE	STANDARD ACTION	YES	E11 – Privileged commands
CREATE PROFILE	STANDARD ACTION	YES	E11 – Privileged commands
CREATE PUBLIC SYNONYM	SYSTEM PRIVILEGE	YES	E13 – Objects
CREATE ROLE	STANDARD ACTION	YES	E7 – Create role
CREATE SQL TRANSLATION PROFILE	SYSTEM PRIVILEGE	YES	E13 – Objects
CREATE USER	SYSTEM PRIVILEGE	YES	E5 – Create user account

Mixed Mode Default Unified Policy ORA_SECURECONFIG			
Audit Option	**Option Type**	**Common**	**Integrigy Framework**
DROP ANY PROCEDURE	SYSTEM PRIVILEGE	YES	E13 – Objects
DROP ANY SQL TRANSLATION PROFILE	SYSTEM PRIVILEGE	YES	E13 – Objects
DROP ANY TABLE	SYSTEM PRIVILEGE	YES	E13 – Objects
DROP DATABASE LINK	STANDARD ACTION	YES	E13 – Objects
DROP DIRECTORY	STANDARD ACTION	YES	E13 – Objects
DROP PLUGGABLE DATABASE	STANDARD ACTION	YES	E11 - Privileged commands
DROP PROFILE	STANDARD ACTION	YES	E14 - Modify configuration settings
DROP PUBLIC SYNONYM	SYSTEM PRIVILEGE	YES	E13 – Objects
DROP ROLE	STANDARD ACTION	YES	E8 - Modify role
DROP USER	SYSTEM PRIVILEGE	YES	E6 - Modify user account
EXEMPT ACCESS POLICY	SYSTEM PRIVILEGE	YES	E14 - Modify configuration settings
EXEMPT REDACTION POLICY	SYSTEM PRIVILEGE	YES	E14 - Modify configuration settings
GRANT ANY OBJECT PRIVILEGE	SYSTEM PRIVILEGE	YES	E9 - Grant/revoke user privileges
GRANT ANY PRIVILEGE	SYSTEM PRIVILEGE	YES	E9 - Grant/revoke user privileges
GRANT ANY ROLE	SYSTEM PRIVILEGE	YES	E9 - Grant/revoke user privileges
LOGMINING	SYSTEM PRIVILEGE	YES	E12 - Modify audit and logging
LOGOFF	STANDARD ACTION	YES	E2 - Logoff
LOGON	STANDARD ACTION	YES	E1 - Login
PURGE DBA_RECYCLEBIN	SYSTEM PRIVILEGE	YES	E11 - Privileged commands
SET ROLE	STANDARD ACTION	YES	E11 - Privileged commands
TRANSLATE ANY SQL	SYSTEM PRIVILEGE	YES	E11 - Privileged commands

For more information on Mixed Mode –

- Oracle Database Security Guide 12c Release 1 http://docs.oracle.com/database/121/DBSEG/auditing.htm#DBSEG493
- Why Mixed Mode is generating log data and how to disable it refer to “The UNIFIED_AUDIT_TRAIL is Getting Populated even if Unified Auditing was not explicitly enabled in 12c” Note ID 1624051.1, Oracle Corporation, 28 March 2014, https://support.oracle.com/rs?type=doc&id=1624051.1

SYS.UNIFIED_AUDIT_TRAIL

Regardless of using either Mixed Mode or Pure Unified Auditing, the table `SYS.UNIFIED_AUDIT_TRAIL` can be used. `SYS.UNIFIED_AUDIT_TRAIL` consolidates all audit activity into a single source. As such, it is an important source of truth for 12c Oracle auditing.

The key column in `SYS.UNIFIED_AUDIT_TRAIL` is `AUDIT_TYPE`. This column shows from which Oracle component the log data originated -

SYS.UNIFIED_AUDIT_TRAIL Component Sources		
Column AUDIT_TYPE Value	**Description**	**Number of Columns in Table**
Standard	Standard auditing including SYS audit records	44
XS	Real Application Security (RAS)and RAS auditing	17
Label Security	Oracle Label Security	14
Datapump	Oracle Data Pump	2
FineGrainedAudit	Fine grained audit(FGA)	1
Database Vault	Data Vault(DV)	10
RMAN_AUDIT	Oracle RMAN	5
Direct path API	SQL*Loader Direct Load	1
	Total	94

For a full description of each column in the table `SYS.UNIFIED_AUDIT_TRAIL`, refer to the Oracle® Database Reference 12*c* Release 1 (12.1) http://docs.oracle.com/database/121/REFRN/refrn29162.htm#REFRN29162

Other Important Unified Audit Features

To complete the survey of new Oracle 12c Unified Audit functionality, the following features should be noted –

Two new roles

Who can define and view audit data is controlled by two new database roles –

- **AUDIT_ADMIN –** This role should be granted only to trusted users. This role allows Unified and Fine-Grained Audit policies to be created and administered, use of the AUDIT and NOAUDIT SQL statements as well as to view audit data.
- **AUDIT_VIEWER –** Typically given to an external or internal auditor this role allows audit data to be viewed and analyzed.

AUDSYS Schema and Improved Performance

Auditing is now implemented within the System Global Area (SGA). This reduces the performance overhead of auditing.

Oracle 12c writes audit data first to the system global area (SGA) queues. Oracle then periodically empties the queues to the `AUDSYS` schema audit table in the `SYSAUX` tablespace. According to the Oracle documentation, this design greatly improves the performance of the audit trail processes and the database as a whole.

There are two queuing modes to write audit data out of the SGA:

- **Immediate-write**: immediately written
- **Queued-Write** (default): periodically dequeued

Audit Policies and Syntax

Key to understanding the benefits of Unified Auditing is the concept of audit policies. A full description of Unified Audit policies can be found here.

Unified Auditing allows multiple audit policies enabled at the same time, however, the number of enabled policies should be minimized. The Unified Auditing policy syntax is designed for one policy to be written that covers all the audit required audit conditions. Oracle recommends to group related options into a single policy instead of creating multiple small policies. This enables easier management of audit policies.

Generic syntax for Unified Auditing policies -

```
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}];
```

As an example, the following policy audits logons by the user APPS using SQL-Plus not from the database server(s) -

```
CREATE AUDIT POLICY logon_pol
ACTIONS LOGON
WHEN 'INSTR(UPPER(SYS_CONTEXT(''USERENV'',''CLIENT_PROGRAM_NAME'')),
      ''SQLPLUS'') > 0'
AND  'SYS_CONTEXT (''USERENV'', ''HOST'') NOT IN
      (''prod_db_rac1'',''prod_db_rac2'')'
EVALUATE PER SESSION;
AUDIT POLICY logon_pol BY APPS;
```

More information can be found on these topics in the 12c Unified Auditing, Oracle Database Security Guide 12c Release 1 (12.1).

Related Oracle 12c Audit Features

Auditing Multitenant (Pluggable Databases)

In a multitenant environment, Oracle 12c audit polices audit policies can be set to be one of the following:

- **Common –** These policies are available to all pluggable databases (PDB)s in the multitenant environment. You can enable common audit policies only for common users, and this type of policy can contain object audit options of only common objects.

- **Local -** These policies apply only to a single pluggable database. By default, audit policies are local to the current PDB.

With regard to pluggable databases, Integrigy's Framework can be implemented locally either to a single pluggable (tenant) database or to all pluggable databases.

For more information on auditing multi-tenant pluggable databases –

- Oracle Database Security Guide 12c Release 1 guide: http://docs.oracle.com/database/121/DBSEG/audit_config.htm#DBSEG634
- Oracle Database Concepts 12*c* Release 1 (12.1) guide: http://docs.oracle.com/database/121/CNCPT/cdbovrvw.htm#CNCPT89234

MANDATORY AUDITING

Certainly from an auditing and logging perspective, the best new feature delivered by Oracle 12c is mandatory auditing of the administrative users such as SYSDBA. This has been described as 'always on auditing'. By default, the following audit related activities are now mandatorily audited -

- CREATE AUDIT POLICY
- ALTER AUDIT POLICY
- DROP AUDIT POLICY
- AUDIT
- NOAUDIT
- EXECUTE of the DBMS_FGA PL/SQL package
- EXECUTE of the DBMS_AUDIT_MGMT PL/SQL package
- All configuration changes that are made to Oracle Database Vault
- ALTER TABLE attempts on the AUDSYS audit trail table (this table cannot be altered)
- Top level statements by administrative users SYS, SYSDBA, SYSOPER, SYSASM, SYSBACKUP, SYSDG, and SYSKM, until the database opens. When the database opens, Oracle Database audits these users using the audit configurations in the system.

The audit activity resulting from mandatory auditing can be found in `SYS.UNIFIED_AUDIT_TRAIL`.

Note when the database is not writable (such as during database mounting), if the database is closed, or if it is read-only, then Oracle writes the audit records to external files in the $ORACLE_BASE/audit/$ORACLE_SID directory.

For more information on mandatory auditing, refer to the Oracle Database Security Guide 12*c* Release 1 Guide: http://docs.oracle.com/database/121/DBSEG/audit_admin.htm#DBSEG361.

Mandatory Auditing	Integrigy Framework Event

Mandatory Auditing	Integrigy Framework Event
▪ CREATE AUDIT POLICY ▪ ALTER AUDIT POLICY ▪ DROP AUDIT POLICY ▪ EXECUTE of the DBMS_FGA PL/SQL package ▪ EXECUTE of the DBMS_AUDIT_MGMT PL/SQL package ▪ All configuration changes that are made to Oracle Database Vault ▪ ALTER TABLE attempts on the AUDSYS audit trail table (remember that this table cannot be altered)	`E12 - Modify audit and logging`
▪ Top level statements by the administrative users SYS, SYSDBA, SYSOPER, SYSASM, SYSBACKUP, SYSDG, and SYSKM until the database opens ▪ AUDIT ▪ NOAUDIT	`E11 - Privileged commands`

Note: Activity and be found in `SYS.UNIFIED_AUDIT_TRAIL` when in pure mode and to the traditional audit trails in mixed mode.

Real Application Security

Oracle 12c introduces Real Application Security (RAS). RAS is the next generation Virtual Private Database (VPD) and is installed with Oracle Enterprise Edition – no additional license required. RAS is a new declarative and granular authorization model and is designed to be an application security platform for end-to-end application security. For those developing APEX applications (also installed with Enterprise Edition), RAS will certainly become an integral tool.

With RAS, developers define security policies instead of having to create and maintain PL/SQL code. Most notably, RAS however extends the security solution to define both application users and roles separate from database users and roles.

RAS allows for the creation of users, complete with user names and passwords, and stores them in the database. RAS users are not stored in DBA_USERS. RAS users are defined in DBA_XS_USERS, and their passwords are stored in SYS. XS$VERIFIERS.

Direct Database Logon

With 12.1.0.1, RAS users can also directly connect to the database. With 12.1.0.2, RAS users can be defined with a flag to allow or disallow direct database logons. As any database security monitoring and logging solution should be monitoring database logon activity, it should be known that RAS users will NOT show up in standard Oracle database auditing. Standard database auditing instead picks up login activity by the generic user XS$NULL. Because it is designed to be part of the application, RAS has its own logging and auditing solution.

Basic logon activity for RAS users, however, is logged in `SYS.UNIFIED_AUDIT_TRAIL`. Even if you have NOT enabled Unified Auditing in 12c, `SYS.UNIFIED_AUDIT_TRAIL` is being populated. If you have compliance requirements to log and audit database logons, you will need to monitor `SYS.UNIFIED_AUDIT_TRAIL` for RAS user activity as well as for the creation of RAS users if not also potentially configuring RAS auditing.

You can test for yourself how standard database auditing logs RAS user logons as follows –

1. Ensure auditing for create session is enabled, if not: audit create session by access;
2. Create Real application security user

```
BEGIN

        XS_PRINCIPAL.CREATE_USER(NAME=>'INTEGRIGY_RAS_USER');
END;
```

3. Set password for Real Application Security user

```
BEGIN
        XS_PRINCIPAL.SET_PASSWORD('INTEGRIGY_RAS_USER','oracle');
END;
```

4. Review both dba_users and dba_xs_users to see for yourself where RAS users are defined.
5. Log into the database with: INTEGRIGY_RAS_USER/oracle
6. Look at your auditing and see a logon from XS$NULL instead of INTEGRIGY_RAS_USER
   select * from sys.aud$ order by 1 desc
7. Now look at `SYS.UNIFIED_AUDIT_TRAIL`. You will see XS$NULL for the DBUSERNAME but you will see 'INTEGRIGY_RAS_USER' in XS_USER_NAME.

```
select dbusername,xs_user_name ,event_timestamp
from SYS.UNIFIED_AUDIT_TRAIL
where xs_user_name = 'INTEGRIGY_RAS_USER'
order by event_timestamp;
```

If you are not familiar with XS$NULL, XS$NULL is created when the database component Oracle XML Database (XDB) is installed. XDB is now a mandatory component of 12c and as such, XS$NULL must exist in the database. XS$NULL is an internal account that represents the absence of a user in a session. It is used by the lightweight session infrastructure for APEX, RAS, and XDB and the name of this user is hard coded in those modules. Because XS$NULL is not really a user, this account can only be accessed by the Oracle Database instance. XS$NULL has no privileges, and no one can authenticate as XS$NULL, nor can authentication credentials ever be assigned to XS$NULL.

For more information on Real Application Security:

- Summary on Oracle.com HTTP://WWW.ORACLE.COM/TECHNETWORK/DATABASE/SECURITY/REAL-APPLICATION-SECURITY/REAL-APPLICATION-SECURITY-1964775.HTML
- Oracle Database Real Application Security Administrator's and Developer's Guide
  12*c* Release 1 (12.1) http://docs.oracle.com/database/121/DBFSG/intro.htm#DBFSG10000

RAS Auditing

Real Application Security administration and run-time actions can be audited by configuring and enabling 12c Unified Auditing policies.

To list what RAS events are available to audit query SYS.AUDITABLE_SYSTEM_ACTIONS –

```
SELECT NAME FROM SYS.AUDITABLE_SYSTEM_ACTIONS WHERE COMPONENT = 'XS';
```

The following static data dictionary views show what audit polices have been defined for RAS –

- DBA_XS_AUDIT_POLICY_OPTIONS - shows auditing options defined for RAS
- DBA_XS_ENB_AUDIT_POLICIES - lists users for whom RAS Unified Audit polices are enabled

RAS audit events can be found in two places –

- SYS.DBA_XS_AUDIT_TRAIL
- SYS.UNIFIED_AUDIT_TRAIL WHERE AUDIT_TYPE = ‘XS’

For information on how to setup and use RAS auditing refer to –

- Oracle Database Security Guide 12c Release 1
  http://docs.oracle.com/database/121/DBSEG/audit_config.htm#DBSEG367

12c Data Dictionary for Auditing

The following table lists the Oracle 12c data dictionary and dynamic views that provide auditing information –

View	Description
ALL_AUDIT_POLICIES	Displays information about all fine-grained audit policies
ALL_DEF_AUDIT_OPTS	Lists default object-auditing options that are to be applied when objects are created
AUDIT_UNIFIED_CONTEXTS	Describes application context values that have been configured to be captured in the audit trail
AUDIT_UNIFIED_ENABLED_POLICIES	Describes all unified audit policies that are enabled in the database
AUDIT_UNIFIED_POLICIES	Describes all unified audit policies created in the database
AUDIT_UNIFIED_POLICY_COMMENTS	Shows the description of each unified audit policy, if a description was entered for the unified audit policy using the COMMENT SQL statement
AUDITABLE_SYSTEM_ACTIONS	Maps the auditable system action numbers to the action names
CDB_UNIFIED_AUDIT_TRAIL	Similar to the UNIFIED_AUDIT_TRAIL view, displays the audit records but from all PDBs in a multitenant environment. This view is available only in the root and must be queried from there.
DBA_AUDIT_POLICIES	Displays information about fine-grained audit policies
DBA_SA_AUDIT_OPTIONS	Describes audited Oracle Label Security events performed by users, and indicates if the user's action failed or succeeded
DBA_XS_AUDIT_TRAIL	Displays audit trail information related to Oracle Database Real Application Security
DV$CONFIGURATION_AUDIT	Displays configuration changes made by Oracle Database Vault administrators
DV$ENFORCEMENT_AUDIT	Displays user activities that are affected by Oracle Database Vault policies
SYSTEM_PRIVILEGE_MAP	Describes privilege (auditing option) type codes. This table can be used to map privilege (auditing option) type numbers to type names.

View	Description
V$LOGMNR_CONTENTS	Contains log history information. To query this view, you must have the SELECT ANY TRANSACTION privilege. Applies to the current PDB only.
V$OPTION	You can query the PARAMETER column for Unified Auditing to find if unified auditing is enabled. If False then is set to Mixed Mode. If True is set to Pure mode which means only the 12c audit configurations will be used. Pure mode ignores pre-12c log and audit configurations.
UNIFIED_AUDIT_TRAIL	Displays all audit records from all audit sources. Is populated in Mixed mode.

Other Auditing Features

Several standard features of the Oracle database should be kept in mind when considering what alerts and correlations are possible when combining Oracle database and application log and audit data.

Client Identifier

Default Oracle database auditing stores the database username but not the application username. In order to pull the application username into the audit logs, the CLIENT IDENTIFIER attribute needs to be set for the application session which is connecting to the database. The CLIENT_IDENTIFIER is a predefined attribute of the built-in application context namespace, USERENV, and can be used to capture the application user name for use with global application context, or it can be used independently.

CLIENT IDENTIFIER is set using the DBMS_SESSION.SET_IDENTIFIER procedure to store the application username. The CLIENT IDENTIFIER attribute is one the same as V$SESSION.CLIENT_IDENTIFIER. Once set you can query V$SESSION or `SELECT SYS_CONTEXT('USERENV','CLIENT_IDENTIFIER') FROM DUAL.`

The table below offers several examples of how CLIENT_IDENTIFIER is used. For each example, for Level 3 alerts, consider how the value of CLIENT_IDENTIFIER could be used to identify network usernames, enterprise application usernames as well as security and electronic door system activity logs.

Oracle CLIENT_IDENTIFIER	
Application	**Application Usage**
Oracle E-Business Suite	As of Release 12, the Oracle E-Business Suite automatically sets and updates CLIENT_IDENTIFIER to the FND_USER.USERNAME of the user logged on. Prior to Release 12, follow Support Note How to add DBMS_SESSION.SET_IDENTIFIER(FND_GLOBAL.USER_NAME) to FND_GLOBAL.APPS_INITIALIZE procedure (Doc ID 1130254.1)

Oracle CLIENT_IDENTIFIER	
Application	**Application Usage**
Oracle PeopleSoft	Starting with PeopleTools 8.50, the PSOPRID is now additionally set in the Oracle database CLIENT_IDENTIFIER attribute.
SAP	With SAP version 7.10 above, the SAP user name is stored in the CLIENT_IDENTIFIER.
Oracle Business Intelligence Enterprise Edition(OBIEE)	When querying an Oracle database using OBIEE the connection pool username is passed to the database. To also pass the middle-tier username, set the user identifier on the session. To do this in OBIEE, open the RPD, edit the connection pool settings and create a new connection script to run at connect time. Add the following line to the connect script: CALL DBMS_SESSION.SET_IDENTIFIER('VALUEOF(NQ_SESSION.USER)')

Example of Unified Audit syntax using `CLIENT_IDENTIFIER` where if the Oracle E-Business user 'mmiller' attempts to delete from the table OE.Orders -

```
CREATE AUDIT POLICY sales_clerk_mm_pol
ACTIONS DELETE ON OE.ORDERS
WHEN 'SYS_CONTEXT(''USERENV'', ''CLIENT_IDENTIFIER'')
       = ''mmiller'''
EVALUATE PER STATEMENT;
AUDIT POLICY sales_clerk_mm_pol by APPS;
```

Database Link Usage

A database link is a one-way connection between two databases. Starting with Oracle version 11.2.0.3, database session information now can report additional information for those sessions involving database links. As often database links are created between databases of different security profiles; it is important to note that it is now able to log session activity that includes the details of the database link.

DBLINK_INFO returns the source of a database link. Specifically, it returns a string of the form –

SOURCE_GLOBAL_NAME=*dblink_src_global_name*
DBLINK_NAME=*dblink_name*
SOURCE_AUDIT_SESSIONID=*dblink_src_audit_sessionid*
where:

- *dblink_src_global_name* is the unique global name of the source database
- *dblink_name* is the name of the database link on the source database
- *dblink_src_audit_sessionid* is the audit session ID of the session on the source database that initiated the connection to the remote database using *dblink_name*

You can verify DBLINK_INFO –

- Oracle 12c provides a DBLINK_INFO column in `SYS.UNIFIED_AUDIT_TRAIL`.
- `SELECT SYS_CONTEXT('USERENV','DBLINK_INFO') FROM DUAL`

Last Login

Tracking when database users last logged in is a common security and compliance requirement. This is required in order to reconcile users and identify stale users. New with Oracle12c, Oracle provides this information for database users. The system table `SYS.DBA_USERS` has a new column, last_login.

```
SELECT USERNAME, ACCOUNT_STATUS, COMMON, LAST_LOGIN
FROM SYS.DBA_USERS
ORDER BY LAST_LOGIN ASC;
```

Username	Account_Status	Common	Last_Login
C##INTEGRIGY	OPEN	YES	05-AUG-14 12.46.52.000000000 PM AMERICA/NEW_YORK
C##INTEGRIGY_TEST_2	OPEN	YES	02-SEP-14 12.29.04.000000000 PM AMERICA/NEW_YORK
XS$NULL	EXPIRED & LOCKED	YES	02-SEP-14 12.35.56.000000000 PM AMERICA/NEW_YORK
SYSTEM	OPEN	YES	04-SEP-14 05.03.53.000000000 PM AMERICA/NEW_YORK

Integrigy Log and Audit Framework

Integrigy's Framework can be implemented either using Unified Auditing in Mixed Mode or in Pure Mode. With regard to pluggable databases, Integrigy's Framework can be implemented either to a single pluggable (tenant) database or to all pluggable databases. The discussion below assumes the use of the Oracle Audit Vault for Level II centralized monitoring.

Integrigy's log and audit Framework can be downloaded here.

Framework with Oracle 12c Mixed Mode Unified Audit

To implement the Framework with Oracle 12c Unified Auditing in Mixed Mode, there is no change. Implement the Framework the same as for Oracle 11gR2. The only exception is that Integrigy recommends to either periodically purge Unified Auditing data being collected by default in `SYS.UNIFIED_AUDIT_TRAIL` or to disable the default Unified Audit policies. To disable the default policy (`ORA_SECURECONFIG)` follow the instructions in this Oracle Support Note: Doc ID 1624051.1. Please note the default policy `ORA_DATABASE_PARAMETER` audits the same events as the 11g default auditing.

Integrigy's Log and Audit Framework can be easily implemented using the Oracle Audit Vault. The high-level summary is a follows:

Level 1
Enable database auditing as directed by the Integrigy Framework Level 1 requirements.

Level 2

1. Install a centralized logging tool such as the Oracle Audit Vault.
2. Configure Oracle database to use Syslog per Integrigy Framework Level 2 requirements. Set the database initialization parameter AUDIT_TRAIL parameter to equal 'OS' and AUDIT_FILE_DEST parameter to desired file in the directory specification. Last set the initialization parameter AUDIT_SYSLOG_LEVEL to 'LOCAL1.WARNING' to generate Syslog formatted log files.
3. If using the Oracle Audit Vault, install and activate the Oracle Audit Vault collector agent OSAUD for operating system files. Collect Syslog formatted logs located by the AUDIT_FILE_DEST parameter.

Level 3
Protect application log and audit tables by creating standard database audit policies and adding these new policies the Audit Vault Collectors. Create database alerts based on correlations between standard database events and application audit logs.

Framework with Oracle 12c Pure Unified Audit

To implement the Integrigy Log and Audit Framework on Oracle 12c using Unified Audit in Pure mode –

Level 1

1. Convert to pure Unified Audit if not already done so
2. If you have enabled auditing prior, and have been using a tool such as Oracle Audit Vault, Splunk or ArcSight you will need disable data collectors for sources such as `SYS.AUD$` or `SYS.FGA_LOG$` tables. These data sources will no longer be populated when using Unified Audit in Pure mode.
3. Enable the following Unified Audit polices:
   - `ORA_SECURECONFIG`
   - `ORA_ACCOUNT_MGMT`
   - `ORA_DATABASE_PARAMETER`

Level 2

1. Point your centralized log collector at `SYS.UNIFIED_AUDIT_TRAIL`.

Level 3

1. Add application log and navigation Application tables
   - Oracle E-Business Suite, SAP, PeopleSoft, Apex and OBIEE
2. If using Real Application Security (RAS), enable standard Unified Audit policies for RAS:
   - `ORA_RAS_POLICY_MGMT`
   - `ORA_RAS_SESSION_MGMT`

References

General

- "Building an Audit Trail in an Oracle Applications Environment," Jeff Hare and Stephen Kost, http://www.integrigy.com/files/Building_an_Audit_Trail_in_an_Oracle_Applications_Environment.pdf
- "Real World Database Auditing," Stephen Kost, Collaborate 2009, Session #602, http://www.integrigy.com/files/IOUG%202009%20-%20Real%20World%20Database%20Auditing.pdf
- "Applied Oracle Security," Knox et al., Oracle Press, 2010
- "Protecting Oracle Database 12c," Paul Wright, Apress 2014

Oracle Documentation

- "Oracle Database Security Guide 12c Release 1 (12.2) E48135-09," Oracle Corporation, July 2014 http://docs.oracle.com/database/121/DBSEG/E48135-09.pdf
- "Oracle Database Reference 12c Release 1 (12.1) E41527-13," Oracle Corporation, August 2014 http://docs.oracle.com/database/121/REFRN/E41527-13.pdf
- "Security and Compliance with Oracle Database 12c," Oracle Corporation, April 2014, http://docs.oracle.com/cd/E23574_01/server.103/e16813.pdf
- "Oracle Database Concepts 12*c* Release 1 (12.1) E41396-10" , Oracle Corporation, August 2014 http://docs.oracle.com/database/121/CNCPT/E41396-10.pdf
- "Oracle Database Real Application Security Administrator's and Developer's Guide 12c Release 1 (12.1) E48189-08," Oracle Corporation, July 2014 http://docs.oracle.com/database/121/DBFSG/E48189-08.pdf

Oracle Support

- "Troubleshooting (Audit Trail)," Oracle Support Note ID 105624.1, Oracle Corporation, 10 December 2013, https://support.oracle.com/rs?type=doc&id=105624.1
- "Auditing How To, Troubleshooting, and Error Message Document," Oracle Support Note ID 1579731.1, Oracle Corporation, 3 September 2013, https://support.oracle.com/rs?type=doc&id=1579731.1
- "Master Note For Oracle Database Auditing," Oracle Support Note ID 1299033.1, Oracle Corporation, 7 January 2014, https://support.oracle.com/rs?type=doc&id=1299033.1
- "Master Note for Oracle Database Fine-Grained Auditing," Oracle Support Note ID 1533543.1, Oracle Corporation, 25 April 2013, https://support.oracle.com/rs?type=doc&id=1533543.1
- "How To Enable The New Unified Auditing In 12c?" Note ID 1567006.1, Oracle Corporation, 23 August 2013, https://support.oracle.com/rs?type=doc&id=1567006.1
- Is the XS$NULL user a required account? (Doc ID 1556725.1) https://support.oracle.com/rs?type=doc&id=1556725.1

About Integrigy

Integrigy Corporation (www.integrigy.com)

Integrigy Corporation is a leader in application security for enterprise mission-critical applications. AppSentry, our application and database security assessment tool, assists companies in securing their largest and most important applications through detailed security audits and actionable recommendations. AppDefend, our enterprise web application firewall is specifically designed for the Oracle E-Business Suite. Integrigy Consulting offers comprehensive security assessment services for leading databases and ERP applications, enabling companies to leverage our in-depth knowledge of this significant threat to business operations.

INTEGRIGY
Integrigy Corporation
P.O. Box 81545
Chicago, Illinois 60681 USA
888/542-4802
www.integrigy.com