INTEGRIGY

WHITE PAPER

Logging SAP, PeopleSoft and E-Business Suite End-Users in Oracle RDBMS Audit Logs

APRIL 2017

Logging SAP, PeopleSoft and E-Business Suite End-users in Oracle RDBMS Audit Logs

Version 1.0 – April 2017 - created

Authors: Mike Miller, CISSP, CISSP-ISSMP, CCSK

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

Table of Contents

LOGGING ERP END-USER ACTIONS IN ORACLE RDBMS AUDIT LOGS

Logging and auditing database connections to application users for SAP, PeopleSoft, and the E-Business Suite is possible with a standard feature of the Oracle RDBMS. SAP, PeopleSoft, and the E-Business Suite all populate a database attribute that is automatically passed to Oracle's native audit logs. This attribute is the CLIENT_ID and within the Oracle dictionary and documentation is also referred to as CLIENTID and CLIENT_IDENTIFIER.

The CLIENT_ID is an application context. Application contexts are name-value pairs that the Oracle Database stores in memory. Consider application contexts as global variables that hold information for the duration of a session; they are not persistent.

The CLIENT_ID context is NOT the same as the CLIENT_INFO context. The essential difference between the two is one contains application's end-user username and is passed to the native Oracle audit logs, and the other holds an abbreviated application log string and is not passed to Oracle's native audit logs.

```
--Example:
SELECT USERNAME, CLIENT_IDENTIFIER, CLIENT_INFO
FROM V$SESSION
WHERE TYPE = 'USER';
```

Technically the CLIENT_INFO is set with the DBMS_APPLICATION_INFO package and is only visible in the V$SESSION view. The CLIENT_ID context is set with DBMS_SESSION.SET_IDENTIFIER and is also visible in the V$SESSION view in the column CLIENT_IDENTIFIER, but more importantly, CLIENT_ID is written out to the following Oracle Audit logs:

- DBA_AUDIT_TRAIL (SYS.AUD$.CLIENTID)
- DBA_FGA_AUDIT_TRAIL.CLIENT_ID (SYS.FGA_LOG$.CLIENTID)
- DBA_COMMON_AUDIT_TRAIL.CLIENT_ID
- V$SESSION.CLIENT_IDENTIFIER

Application	Example of how CLIENT_IDENTIFIER is used
PeopleSoft	Starting with PeopleTools 8.50, the PSOPRID (SYSADM.PSOPRDEFN.OPRID) is now additionally set in the Oracle database CLIENT_IDENTIFIER attribute if the parameter EnableDBMonitoring is set to a value of 1 within the PSAPPSRV.cfg configuration file.
Oracle E-Business Suite	As of Release 12, the Oracle E-Business Suite automatically sets and updates CLIENT_IDENTIFIER to the APPLYSS.FND_USER. USER_NAME of the user logged on. Before 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) For 12.2 the profile option FND: Connection Tagging (FND_CONNECTION_TAGGING) must be first enabled – it is by default.

Application	Example of how CLIENT_IDENTIFIER is used
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's username is passed to the database. To also pass the middle-tier username, set the user identifier in the session. Edit the RPD 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)')

Oracle Audit Trails			
Session Attribute (V$SESSION)	**Description**	**Traditional Auditing (SYS.AUD$)**	**Fine Grained Auditing (SYS.FGA_LOG$)**
CLIENT_IDENTIFIER	End user username	CLIENTID	CLIENTID
CLIENT_INFO	Concatenated application log string	Not passed	Not passed
MODULE	ABAP program, module, application component or service	Not passed	Not passed
ACTION	Business action being executed, page, code event, location within program	Not passed	Not passed

Program Name

The program name attribute (V$SESSION.PROGRAM) is not by default passed to Oracle's audit logs. It can be optionally included. To do so, apply Patch 7023214 on the source database. After the patch is applied, the following event needs to be set:

```
ALTER SYSTEM SET
          EVENT='28058 trace name context forever'
          COMMENT='enable program logging in audit trail' SCOPE=SPFILE;
```

For more information, refer to:
How to make the client Program Name appear in Audit Vault reports? (Doc ID 1465610.1)
https://support.oracle.com/rs?type=doc&id=1465610.1

Security and Spoofing

Oracle Database session information includes database user name, operating system user name, host, terminal, IP address, module, program, timestamps, session ID, and other details. These values are critical to auditing and identifying the actual end-user. Many of the database session values can be "spoofed" by an attacker either to mask their true identity or to circumvent security and auditing measures.

For more information refer to:
https://www.integrigy.com/security-resources/analysis/Integrigy_Spoofing_Oracle_Session_Information.pdf/view

PeopleSoft

To utilize the CLIEND_ID context with PeopleSoft, within the PSAPPSRV.cfg configuration file, the parameter EnableDBMonitoring must be set to a value of 1. To utilize the MODULE and ACTION fields in V$SESSION, the parameter EnableAEMonitoring must as well be set to a value of 1 in PSAPPSRV.cfg.

The view V$SESSION holds a concatenated string of application log data. This string is NOT passed to the Oracle audit logs, but still can be useful. The table below documents the major usages of CLIENT_INFO.

For more information: http://preview.tinyurl.com/kh6r7ke

Connection Type	CLIENT_INFO Column in V$SESSION (not passed to audit logs)
2 Tier Connection	oprid, osusername, machinename ,executable,
Application Server Process	oprid, osusername, machinename, tuxedo_domain, executable
3 Tier Connections	oprid, osusername, machinename, tuxedo_domain, executable
PIA (Browser)	oprid, osusername, machinename, tuxedo_domain, executable
Process Scheduler	oprid, osusername, machinename, executable
SQR Connection	oprid, spid
COBOL	oprid, osusername, machinename, executable

Oracle E-Business Suite

The profile option FND: Connect Tagging (FND_CONNECTION_TAGGING) is enabled by default. This feature will log end-user activity to V$SESSION for use in monitoring and logging. When enabled, the detailed end-user activity can be easily passed to the Oracle Audit Vault as well as enhance the capabilities of the Oracle Database Vault.

For more information
https://docs.oracle.com/cd/E26401_01/doc.122/e22952/T156458T663758.htm

Attribute	Passed to Audit Logs	Description
CLIENT_IDENTIFIER	Yes	APPLSYS.FND_USER.USER_NAME using the session. For FNDLOAD and/or FNDCPASS a static value of SYSADMIN is used.
CLIENT_INFO	No	End user attributes for organization, currency, and language

Attribute	Passed to Audit Logs	Description
MODULE	No	Currently executing module
ACTION	No	Currently executing business action

SAP

With version 7.10 above SAP makes use of V$SESSION attributes.

For more information:
https://assets.cdn.sap.com/sapcom/docs/2016/07/925b9298-7e7c-0010-82c7-eda71af511fa.pdf

Attribute	Passed to Audit Logs	Description
CLIENT_IDENTIFIER	Yes	SAP User (e.g. USR01, USER402 etc…)
CLIENT_INFO	No	connection:transaction:mainprogram
MODULE	No	ABAP program name
ACTION	No	Location of statement within the module

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 PeopleSoft. 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