

WHITE PAPER

Automate Reconciliation of Ticket Numbers Using Client Id in Oracle Database Audit Streams

APRIL 2017

AUTOMATE RECONCILIATION OF TICKET NUMBERS USING CLIENT IN ORACLE DATABASE AUDIT STREAMS

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.

Copyright © 2017 Integrigy Corporation. All rights reserved.

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.

Integrigy, AppSentry, and AppDefend are trademarks of Integrigy Corporation. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Table of Contents

- OVERVIEW OF CLIENT ID4**
- How to Implement Client Id..... 5
- How To Use Client Id 6
- ABOUT INTEGRITY8**

OVERVIEW OF CLIENT ID

Reconciling database events to ticket numbers is a time consuming manual task that can be easily automated. The solution is to populate the client_id context variable that is a standard feature of the Oracle RDBMS. Once set, the Client_id is written to the Oracle audit logs for any auditing activity generated during that session. By having the ticket id within the audit logs, reconciliation can be easily automated.

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 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 that 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\$)
- DBA_FGA_AUDIT_TRAIL (SYS.FGA_LOG\$)
- DBA_COMMON_AUDIT_TRAIL

The CLIENT_IDENTIFIER attribute is used in a number of enterprise products. See the table below.

Application	Example of how CLIENT_IDENTIFIER is used
PeopleSoft	Starting with PeopleTools 8.50, the PSOPRID is now additionally set in the Oracle database CLIENT_IDENTIFIER attribute.
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)
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 on 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)')

HOW TO IMPLEMENT CLIENT ID

Best practice is to create a simple function for developers and staff members to call. Below is a sample function and test code:

```
--do not create function this as system. Too many privs if abused.
create or replace function xxxx_ticket(av_ticket_no varchar2, av_desc varchar2)
return varchar2 AUTHID CURRENT_USER
AS lv_string varchar2(100);
BEGIN
--note reports in can be written to key off the static text: ticket_number=
lv_string := 'ticket_no='||av_ticket_no||' Desc:'||av_desc;
lv_string := substr(lv_string,1,64);
DBMS_SESSION.SET_IDENTIFIER(lv_string);
return 'Set';

exception when others then
return 'Ticket Not set';

END;

-- grant to public
grant execute on XXXX_ticket to public;

-- create public synonym. Might need to be APPS or System to create this
create or replace public synonym XXXX_ticket for XXXX.XXXX_ticket;

-- ***** Test the function *****

-- record ticket 123 as being used
select XXXX_ticket('INC123','A good reason') from dual;

-- you will not see it here
select client_identifier
FROM v$session WHERE auid = userenv('sessionid');

-- you will see it here
SELECT SYS_CONTEXT ('USERENV', 'CLIENT_IDENTIFIER') FROM DUAL;

-- force FGA policy (if using FGA)
example: select * from XXXXaud.XXXX_apps_logons_t

-- see ticket 123 in FGA audit log
select clientid, ntimestamp#
from sys.fga_log$ order by ntimestamp# desc
```

HOW TO USE CLIENT ID

Train DBAs and developers before issuing any major change to call the function

For example:

1. The DBA has been assigned ticket number 777 to create a user 'TEST_USER77'
2. The DBA logs on and identifies the session for ticket 777 e.g. `select xxxx_ticket('777') from dual;`
3. The user is created and standard auditing logs both the event and ticket 777 for the event
4. The internal auditor then searches in Splunk for 777 to confirm the event
5. See figure 1 below for a screen of this occurring within Splunk. Figure 2 shows client Id activity within Oracle Audit Vault Database Firewall

Other scenarios:

- Log production usage of APPS or APPS-READ-ONLY for production support. Each session in production where an employee is using APPS could have a corresponding client id to justify the usage of APPS or another equally powerful read-any-table account
- Log production usage of SYSTEM and DBA account activity
- Log code push where database objects and/or users are being created, altered or dropped
- Log data fixes

Possible reports and usages of Client Id:

- Audit activity without client Id (where set to null)
- Report for creation or alteration of user account by client id
- Report listing EBS APPS in session by client_id and without client_id(where null)

Figure 1 Ticket 777 for User Creation

The screenshot shows the Splunk Search & Reporting interface. At the top, there is a search bar with the text 'New Search' and 'ticket_no=777'. Below the search bar, there are several error messages. The main search results show a table with one event. The event details are expanded, showing a table of fields and values. A red circle highlights the search input, and another red circle highlights the 'ticket_no=777' field in the event details. A red arrow points from the search input to the event details.

Type	Field	Value	Actions
Selected	host	192.168.2.12	
	source	udp:514	
	sourcetype	oracle_syslog	
Event	ACTION	51	
	DBID	960448225	
	ENTRYID	4	
	NAME	CREATE USER	
	OBJ_NAME	TEST_USER77	
	OS_USERID	michaelmiller	
	PRIV_USED	20	
	RETURNCODE	0	
	SESSIONID	12043960	
	SES_LABEL	ticket_no=777	
	STATEMENT	88	

Figure 2 - Example of Client Id in Oracle AVDF

The screenshot shows the Oracle Audit Vault Server interface. The main content area displays a report titled 'Demo Clientid with Ticket ID Report'. The report includes a search bar and a table of audit events. The table has columns for Event Time, Event Name, Target Object, Event Status, User Name, OS User Name, and Client Host Name. Red circles highlight the 'clientid=ticket_no=123' field in the 'Client Host Name' column for three events.

Event Time	Event Name	Target Object	Event Status	User Name	OS User Name	Client Host Name
3/23/2015 4:32:51 PM	SELECT	TEST_FGA_POLICY	SUCCESS		skost	INTEGRIGY-WIN7 clientid=ticket_no=123; sessionid=273674621; process#=57823; entryid=9-
3/18/2015 11:46:08 AM	LOGOFF BY CLEANUP		SUCCESS		skost	INTEGRIGY-WIN7 clientid=ticket_no=123; sessionid=273537599; process#=67530; entryid=5-; terminal=unknown
3/18/2015 11:41:14 AM	SELECT	TEST_FGA_POLICY	SUCCESS		skost	INTEGRIGY-WIN7 clientid=ticket_no=123; sessionid=273537599; process#=67530; entryid=4-

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 Corporation

P.O. Box 81545

Chicago, Illinois 60681 USA

888/542-4802

www.integrigy.com