INTEGRIGY

WHITE PAPER

Oracle Database Data Definition Language (DDL) Auditing

APRIL 2017

ORACLE DATA DEFINITION LANGUAGE (DDL) AUDITING

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

DATA DEFINITION LANGUAGE (DDL) LOGGING

Relational databases use DDL statements to define structures such as tables to store data and functions to store code. Monitoring, auditing and logging changes to DDL are key components of a database security program, especially when supporting Enterprise Resource Planning (ERP) solutions such as SAP, PeopleSoft, and the Oracle E-Business Suite. For more information on a comprehensive approach to database auditing refer to the Integrigy whitepaper referenced in the section below on standard auditing.

The options for DDL auditing include:

- Standard auditing
- System Triggers
- Oracle Database Lifecycle Management Pack
- Third party tools such as Imperva and Guardium

STANDARD AUDITING

Standard Oracle auditing can capture changes to DDL and write them to SYS.AUD$. This is the recommended option for DDL auditing because it is the most straightforward and easiest means of auditing DDL and has the advantage tight and prebuilt integration with other Oracle solutions such as the Oracle Audit Vault.

To enable standard database auditing, the startup parameter audit_trail must be set to a value of something other than NONE. Once enabled, audit logs can be written either to the database or Syslog. Examples below show how DDL auditing can be configured:

```
AUDIT TABLE BY ACCESS;
AUDIT VIEW BY ACCESS;
AUDIT PROCEDURE BY ACCESS;
```

Once enabled audit logs can be read in the following tables and system views:

```
DBA_AUDIT_TRAIL (SYS.AUD$)
DBA_COMMON_AUDIT_TRAIL
```

For more information on standard auditing and how to configure it, refer to the following Integrigy whitepaper:
https://www.integrigy.com/security-resources/integrigy-guide-database-auditing-and-logging

SYSTEM TRIGGERS

While recommended for a comprehensive security program, standard auditing is not always used. Sometimes this is because of misconceptions about the performance impact of standard auditing.

To use System Triggers to log DDL changes the steps are as follows:

1. Create a system trigger (e.g. CREATE OR REPLACE TRIGGER <XXX_YOUR_DDL_TRG> AFTER DDL)
2. When the trigger is fired, write DDL changes to a custom table

ORACLE DATABASE LIFECYCLE MANAGEMENT PACK

Another means of auditing DDL with standard Oracle RDBMS functionality is to utilize the Database Lifecycle Management Pack. This feature is not enabled by default because it requires an additional license. When enabled, it writes DDL changes to either the alert log (Oracle 11g) or a DDL specific log (Oracle 12c).

To determine if the Database Lifecycle Management Pack is enabled, use the following SQL:

```
SELECT * FROM V$PARAMETER
WHERE NAME LIKE 'enable_ddl_logging';
```

Per the Oracle documentation, when **ENABLE_DDL_LOGGING** is set to **TRUE** will log following DDL statements executed in a database and write them to the respective log file depending on if you are running 11g or 12c:

ALTER/CREATE/DROP/TRUNCATE CLUSTER
ALTER/CREATE/DROP FUNCTION
ALTER/CREATE/DROP INDEX
ALTER/CREATE/DROP OUTLINE
ALTER/CREATE/DROP PACKAGE
ALTER/CREATE/DROP PACKAGE BODY
ALTER/CREATE/DROP PROCEDURE
ALTER/CREATE/DROP PROFILE
ALTER/CREATE/DROP SEQUENCE
CREATE/DROP SYNONYM
ALTER/CREATE/DROP/RENAME/TRUNCATE TABLE
ALTER/CREATE/DROP TRIGGER
ALTER/CREATE/DROP TYPE
ALTER/CREATE/DROP TYPE BODY
DROP USER
ALTER/CREATE/DROP VIEW

How to use

To utilize the Database Lifecycle Management Pack, the system must be altered:

```
ALTER SYSTEM SET ENABLE_DDL_LOGGING=TRUE;
```

For Oracle 11g DDL log activity is written to the Alert log:

The location of the alert log can be found here:

```
SELECT VALUE FROM V$PARAMETER WHERE NAME='background_dump_dest';
```

Also, starting with 11gR2, it is possible to monitor both the Alert and Listener logs using the system view `V$DIAG_ALERT_EXT`. To query just the alert.log:

```
SELECT * FROM SYS.V$DIAG_ALERT_EXT WHERE TRIM(COMPONENT_ID)='rdbms';
```

Oracle rewrote DDL logging with 12c and now maintains dedicated DDL logs in two files (XML and plain text) located in the $ADR_HOME:

XML Version:
`$ADR_BASE/diag/rdbms/${DBNAME}/${ORACLE_SID}/log/ddl/log.xml`

Plain Text Version:

```
$ADR_BASE/diag/rdbms/${DBNAME}/${ORACLE_SID}/log/ddl_${ORACLE_SID}.log
```

THIRD PARTY TOOLS

Some third party tools can audit DDL. These solutions do not depend on native Oracle RDBMS features and instead depend on agents placed on the database server(s) and/or network taps to intercept network packets going to the database. Once intercepted, the packets are parsed, and DDL statements can be logged.

The advantages of using third party tools include being able to log and audit for most any database platform (e.g. Oracle, MS SQL-Server, DB2, MySQL etc….) and not needing to configure large numbers of Oracle databases for native auditing. Third party tools also allow for a potentially much stronger segregation of duties between DBAs and access to both the audit solution and the audit data. The disadvantages of using such tools are their cost. Such tools are usually deployed to audit a large number of databases where economies of scale can be achieved.

Imperva
https://www.imperva.com/Products/SecureSphereforData

IBM Guardium
http://www-03.ibm.com/software/products/en/ibm-security-guardium-data-activity-monitor

McAfee
https://www.mcafee.com/us/products/data-center-security-suite-for-databases.aspx

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