July, 2016

# Omega Core Audit ™

For Oracle Database

# OMEGA Core Audit

For Oracle Database

## Evaluation Guide

**2.8.1**

www.dataplus-al.com

TABLE OF CONTENTS

# 1 Introduction

## 1.1 About this Evaluation Guide

This guide is intended to shortly explain the functionalities of the Omega Core Audit for Oracle, once Omega Core Audit has been deployed. This is performed using a database evaluation environment, a set of audit/protection policies created for the evaluation and also a benchmarking application.

Instructions for deploying Omega Core Audit are outlined into the Omega Core Audit Deployment Guide. Common instructions are found into the Omega Core Audit User's Guide. Also carefully read the Architecture topic on the Omega Core Audit User's Guide or Deployment Guide.

## 1.2 Functionalities Evaluated

The Omega Core Auditing top functionalities (and evaluated in this guide) are:

**Access Control**
Evaluated is the database entrance mandatory access control on all connections to the database. This is tested by the Logon test option of the Benchmark software.

**Standard Audit**
Evaluated is the auditing of the system for user activity, user statements and operations on objects. This is tested by all testing options.

**Real-Time Protection DDL**
Evaluated is the Structural Change DDL (Data Definition Language – CREATE, ALTER, GRANT, DROP…) audit and protection. This is tested by the DDL test option.

**Real-Time Protection DML**
Evaluated is the Information Change DML (Data Manipulation Language – SEL, INS, DEL, UPD) audit and protection. This is tested by the DML test option.

## 1.3 General Prerequisites

Before the benchmark testing for evaluation, the following requirements must have been met:

- Omega Core Audit must have been installed successfully.
- The Omega Core Audit advised After Install actions must have been committed.
- The database evaluation environment must have been installed.
- The evaluation policies must have been installed.

## 1.4 Omega Core Audit Evaluation Package

Omega Core Audit comes with a full Evaluation Package which is comprised of:

- A database evaluation environment, sample database users and objects.
- Policies created for the evaluation.
- A benchmarking application that generates database activity for the evaluation.

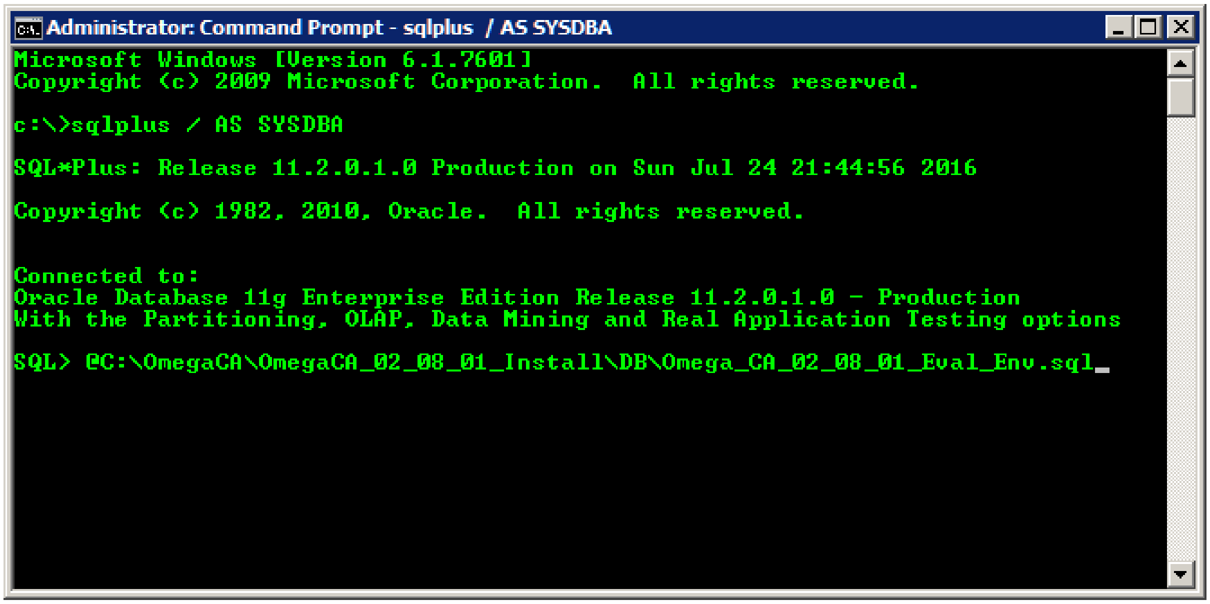
### 1.4.1 Database Evaluation Environment

The database evaluation environment consists of Oracle database accounts and objects created, simulating in miniature the classical infrastructure: a common Application Schema Owner (containing application data, code logic and working in DB in behalf of all application users), two Developer (privileged) Users and one DBA User. There are two tables DEPT for Department and EMP for Employees.

**Install**

To install the database evaluation environment, execute the script:

Omega_CA_[VS]_[MN]_[PT]_Eval_Env.sql.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\>sqlplus / AS SYSDBA

SQL*Plus: Release 11.2.0.1.0 Production on Sun Jul 24 21:44:56 2016

Copyright (c) 1982, 2010, Oracle.  All rights reserved.


Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL> @C:\OmegaCA\OmegaCA_02_08_01_Install\DB\Omega_CA_02_08_01_Eval_Env.sql
```

To install, pres Enter at the point shown in the figure above!

Check the Omega_CA_[VS]_[MN]_[PT]_Eval_Env.log file, there should be no ORA- errors.

This script will install the following into the database:

| | |
|---|---|
| OMEGACATESTAPP01 | Application Schema Owner |
| OMEGACATESTDEV01 | First Developer User |
| OMEGACATESTDEV02 | Second Developer User |
| OMEGACATESTDBA01 | DBA User |

Objects will be created for OMEGACATESTAPP01 Application Owner and sample data will be inserted. These objects you will notice on the Simulator Application.

Privileges on the OMEGACATESTAPP01's objects are granted to the two Developers OMEGACATESTDEV01 and OMEGACATESTDEV02. OMEGACATESTDBA01 is granted the Oracle DBA Role. Other necessary system privileges grants are given to the accounts above to perform the test commands.

## Uninstall

There is no uninstalling routine for the evaluation environment, as the current one is dropped (if existing) on every new install.

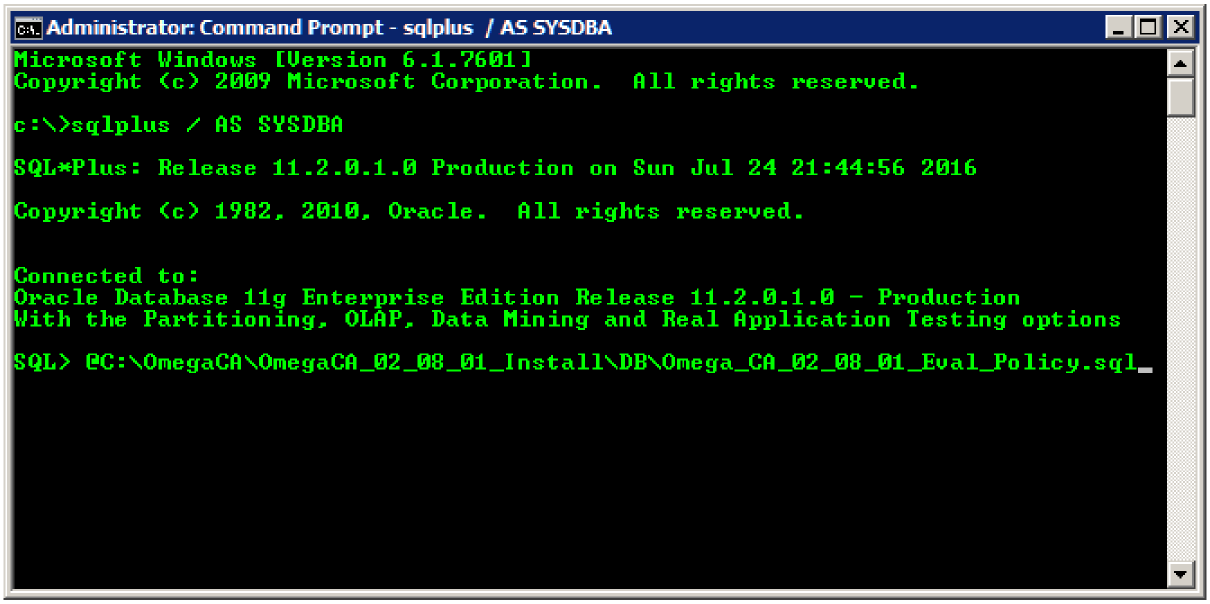
### 1.4.2 Evaluation Policies

Policies created purposely for the evaluation are available as an install routine, rather than entering them manually from the Omega Core Audit Application.

**Install**

To install the evaluation policies into the Omega Core Audit Repository, execute the script:

Omega_CA_[VS]_[MN]_[PT]_Eval_Policy.sql.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\>sqlplus / AS SYSDBA

SQL*Plus: Release 11.2.0.1.0 Production on Sun Jul 24 21:44:56 2016

Copyright (c) 1982, 2010, Oracle.  All rights reserved.


Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL> @C:\OmegaCA\OmegaCA_02_08_01_Install\DB\Omega_CA_02_08_01_Eval_Policy.sql_
```

To install, pres Enter at the point shown in the figure above!

Check the Omega_CA_[VS]_[MN]_[PT]_Eval_Policy.log file, there should be no ORA- errors.

This script will create the following evaluation policies into the Omega Core Audit Repository:

| | |
|---|---|
| Access Control: | “EVL Application Access”, “EVL Developer Access”, “EVL DBA Access” and “EVL Oracle Internals”. |
| Standard Audit: | “EVL Developer Audit”, “EVL App Obj Audit” and “EVL DBA Audit”. |
| RTP DDL: | “EVL Application DDls” and “EVL Security Privileges”. |
| RTP DML: | “EVL Application DMLs”. |

**Important Notes:**

1. All evaluation policies are created as Inactive, so are the Rules and Conditions. You will manually activate them during this evaluation guide.
2. All evaluation policies are created with a prefix of “EVL” (for evaluation) in their name and description.
3. Where Client Host Factor is used, the provided value of <DOMAIN\HOST> should be set to the Benchmark machine name in the format above (also remove <> brackets). Sole exception is on Access Control “EVL Oracle Internals”, where the provided value of <DB-SRV> should be set (without DOMAIN\ and <>) to the Oracle Database machine name. Both the above are shown in the unified trail, field “Userhost”!
4. You can easily convert these evaluation policies to real-life cases.

### Uninstall

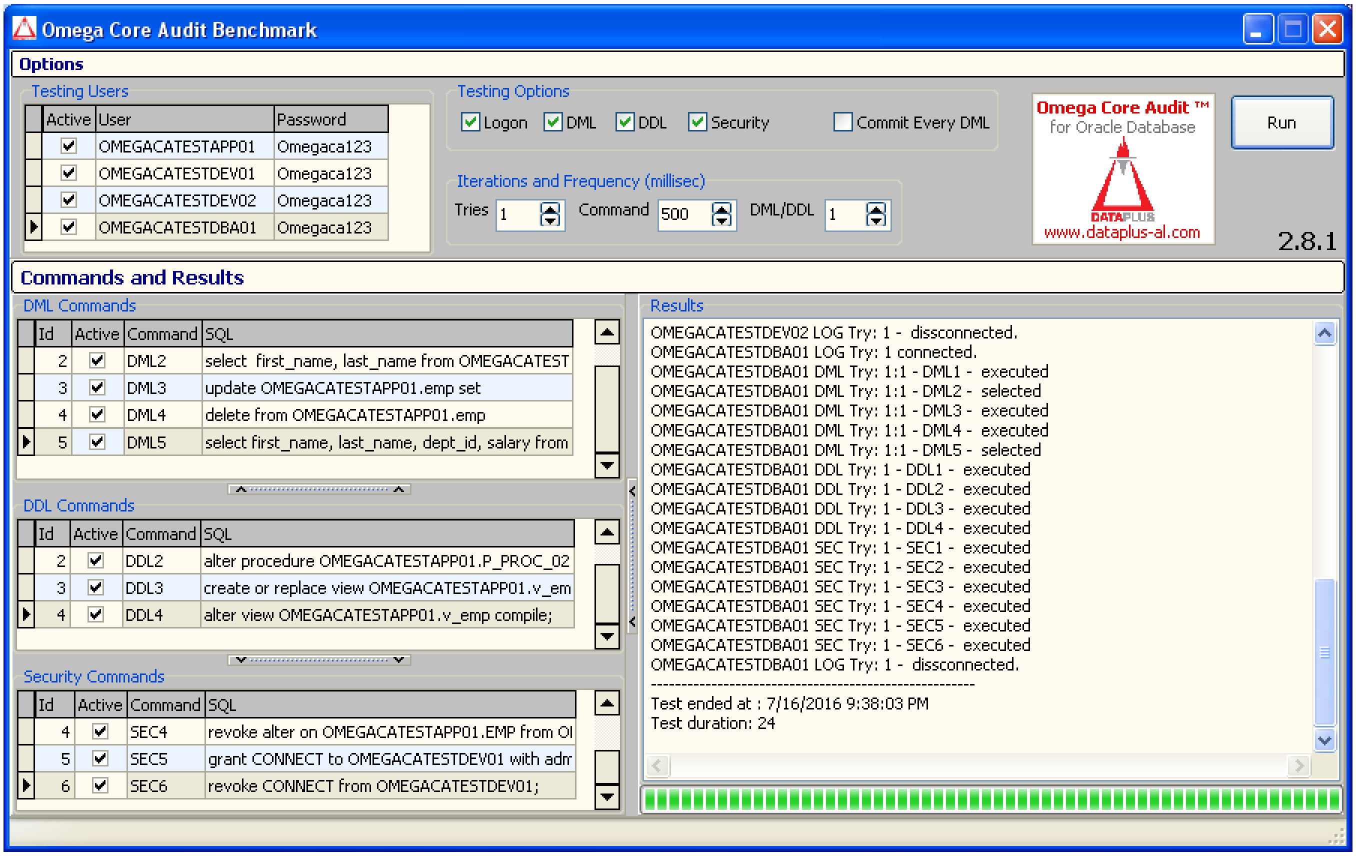
There is no uninstalling routine for the evaluation policies, but you can delete them in the Policy forms of Omega Core Audit’s each module.

### 1.4.3 Omega Core Audit Benchmark

This software has been purposely written for testing and benchmarking the Omega Core Audit solution.

The Omega Core Audit Benchmark generates database activity related to the evaluation environment and evaluation policies, allowing the testing of all four important modules above.

Technology used is the same as that of the Omega Core Audit Application and so is connection to the DB server via Oracle client.



Testing Users

| Active | User | Password |
|---|---|---|
| ☑ | OMEGACATESTAPP01 | Omegaca123 |
| ☑ | OMEGACATESTDEV01 | Omegaca123 |
| ☑ | OMEGACATESTDEV02 | Omegaca123 |
| ☑ | OMEGACATESTDBA01 | Omegaca123 |

Testing Options

☑ Logon ☑ DML ☑ DDL ☑ Security □ Commit Every DML

Iterations and Frequency (millisec)

Tries 1 Command 500 DML/DDL 1

DML Commands

| Id | Active | Command | SQL |
|---|---|---|---|
| 2 | ☑ | DML2 | select  first_name, last_name from OMEGACATEST |
| 3 | ☑ | DML3 | update OMEGACATESTAPP01.emp set |
| 4 | ☑ | DML4 | delete from OMEGACATESTAPP01.emp |
| 5 | ☑ | DML5 | select first_name, last_name, dept_id, salary from |

DDL Commands

| Id | Active | Command | SQL |
|---|---|---|---|
| 2 | ☑ | DDL2 | alter procedure OMEGACATESTAPP01.P_PROC_02 |
| 3 | ☑ | DDL3 | create or replace view OMEGACATESTAPP01.v_em |
| 4 | ☑ | DDL4 | alter view OMEGACATESTAPP01.v_emp compile; |

Security Commands

| Id | Active | Command | SQL |
|---|---|---|---|
| 4 | ☑ | SEC4 | revoke alter on OMEGACATESTAPP01.EMP from Ol |
| 5 | ☑ | SEC5 | grant CONNECT to OMEGACATESTDEV01 with adr |
| 6 | ☑ | SEC6 | revoke CONNECT from OMEGACATESTDEV01; |

Results

```
OMEGACATESTDEV02 LOG Try: 1 -  dissconnected.
OMEGACATESTDBA01 LOG Try: 1 connected.
OMEGACATESTDBA01 DML Try: 1:1 - DML1 -  executed
OMEGACATESTDBA01 DML Try: 1:1 - DML2 -  selected
OMEGACATESTDBA01 DML Try: 1:1 - DML3 -  executed
OMEGACATESTDBA01 DML Try: 1:1 - DML4 -  executed
OMEGACATESTDBA01 DML Try: 1:1 - DML5 -  selected
OMEGACATESTDBA01 DDL Try: 1 - DDL1 -  executed
OMEGACATESTDBA01 DDL Try: 1 - DDL2 -  executed
OMEGACATESTDBA01 DDL Try: 1 - DDL3 -  executed
OMEGACATESTDBA01 DDL Try: 1 - DDL4 -  executed
OMEGACATESTDBA01 SEC Try: 1 - SEC1 -  executed
OMEGACATESTDBA01 SEC Try: 1 - SEC2 -  executed
OMEGACATESTDBA01 SEC Try: 1 - SEC3 -  executed
OMEGACATESTDBA01 SEC Try: 1 - SEC4 -  executed
OMEGACATESTDBA01 SEC Try: 1 - SEC5 -  executed
OMEGACATESTDBA01 SEC Try: 1 - SEC6 -  executed
OMEGACATESTDBA01 LOG Try: 1 -  dissconnected.
-----------------------------------------------------
Test ended at : 7/16/2016 9:38:03 PM
Test duration: 24
```

The application's main form contains two panels:

Options Benchmark options for Testing Users, Testing Options and Iterations
Commands and Results DML and DDL commands used for testing and Result output on the right

**Testing Users**

These are the four users of the database evaluation environment above. Check at least one Active user to perform testing.

**Testing Options**

This GroupBox contains the following Checkbox options:

Logon Generates logon/logoff activity for the benchmarking of the Access Control and Standard Audit modules. When checked, a connection will be opened and closed for each round of commands; otherwise a persistent connection will be opened for all user commands.

DML Generates DML activity for the benchmarking of the Standard Audit and Real-Time Protection DML modules.

DDL Generates DDL activity for the benchmarking of the Standard Audit and Real-Time Protection DDL modules.

Security Generates security activity (Grants/Revokes) for the benchmarking of the Standard Audit and Real-Time Protection DDL modules.

Commit Every DML Commits every DML command performed.

**Iterations and Frequency**

This GroupBox contains the following options:

Tries Number of tries the set of Benchmarking commands (Logon, DML and DDL) are run as a whole for each user.

Command Pause in milliseconds on each command, default 500, should be higher for real-conditions, but can be set lower (or 0) for hard-benchmarking!

DML/DDL The ratio number of times DML Set will be repeated versus the one DDL set. Default 1 set (for testing purposes), but to simulate real conditions DML ratio should be much higher.

**DML Commands**

The DML Commands grid contains the DML commands used in this Benchmark testing. Check at least one Active command if DML benchmarking.

**DDL Commands**

The DDL Commands grid contains the DDL commands used in this Benchmark testing. Check at least one Active command if DDL benchmarking.

**Run Button**

Press the run button to initialize the benchmark testing with the options above!

**Results**

This memo shows the output of benchmarked commands.

## 1.5 Evaluation Reminders

1. The evaluation described later in this guide is cumulative, so while testing the current module, the settings of the previous one remain, so you will see unified trail records of different Policy Type field values. To simplify testing, when searching unified trails, set the Policy Type Search Option field to see only records produced by the module being currently evaluated.

2. The evaluations performed below in this guide are exercised by keeping the default value of Tries = 1 (one try per user)! This parameter logically impacts in proportion the number of trail records produced - frequently referred to below in this guide.

3. The Benchmark application might “freeze” during testing and long operations, but it will be working instead. Please wait until the operation completes and do not interrupt!

4. For immediate results of Standard Audit and Real-Time Protection DML activity on unified trail, manually invoke the DB Audit Trails Purge procedure by going into the main menu Administration, opening form System Components, tab DB Audit Trails Purge and pressing the button Manual Collect.

# 2 Evaluating the Access Control

This chapter is a walkthrough on the Access Control module implementation administered through the Omega Core Audit Application and benchmarked via the Omega Core Audit Benchmark software.

## 2.1 Prerequisites

- The Access Control Module has been activated
- The Access Control Module remains in Silent mode (default in install).
- The ADMINISTER DATABASE TRIGGER System Privilege has been revoked from the Oracle roles DBA and IMP_FULL_DATABASE.

## 2.2 Benchmark Testing

### 2.2.1 Initialization

Rationale:
Access Control Module is activated in Silent mode and there is yet no Active Policy.

In the Omega Core Audit Benchmark software, Testing Options group, check only the Logon Checkbox. Check all the four Users.

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.

In Omega Core Audit, search the unified trail. You will see an Access Control trail record (Policy Type equal to Access Control) generated for each testing user. In the Record Details view, see the Trail Evaluation field for each record. It will be empty because there is no policy activated yet. The logons in the Benchmark have been successful only because the whole Access Control Module is in Silent mode (module's specific feature and default on install). Although no policy created yet, it is a specific behavior of the Access Control module that when non-compliant (i.e. no policy evaluated TRUE for whatever reason, even non-existing or all Inactive) a trail record is created.

**Note**
You should also see Access Control trail records for SYS (and optionally SYSMAN and DBSNMP). These are Oracle own schemas, coming from the local host, usually performed through jobs. They will be treated later in this chapter, topic "Access Control for Oracle Connections"

### 2.2.2 Access Control for Application Schema Owner

Rationale:
The "EVL Application Access" policy establishes a secure logon channel for the Application Schema Owner connections. Policy is created with User Appliance of type "Users Apply" for user OMEGACATESTAPP01 only.

In Omega Core Audit open the Access Control policy "EVL Application Access". Open its only rule "App Owner Access". Activate the two Operand Conditions of Session User and Client Host. For the later set the right "Operand 1" value instead of the provided <DOMAIN\HOST>. Activate the rule "App Owner Access". Activate the policy "EVL Application Access".

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.

In Omega Core Audit, search the unified trail. You will see an Access Control trail record generated for each testing user. In the Record Details view, see the Trail Evaluation field for each record. It will have a value only for the trail record of the OMEGACATESTAPP01 user and empty for the other three. The policy name will be "EVL Application Access". The policy Result will be TRUE.

### 2.2.3 Access Control for Developers

Rationale:
The "EVL Developer Access" policy establishes a secure logon channel for the two Developer Users. Policy is created with User Appliance of type "Users Apply" for users OMEGACATESTDEV01 and OMEGACATESTDEV02.

In Omega Core Audit open the Access Control policy "EVL Developer Access". Open its rule "Developer 01 Access". Activate the two Operand Conditions of Session User and Client Host. For the later set the right "Operand 1" value instead of the provided <DOMAIN\HOST>. Activate the rule "Developer 01 Access". Activate the policy "EVL Developer Access".

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.

In Omega Core Audit, search the unified trail. You will see an Access Control trail record generated for each testing user. In the Record Details view, see the Trail Evaluation field for each record. It will have a value even for the trail record of the OMEGACATESTDEV01 user and empty for the other two. The policy name will be "EVL Developer Access". The policy Result will be TRUE.

Open the rule "Developer 02 Access". Activate the two Operand Conditions of Session User and Client Host. For the later set the right "Operand 1" value instead of the provided <DOMAIN\HOST>. Activate the rule "Developer 02 Access".

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.

In Omega Core Audit, search the unified trail. You will see an Access Control trail record generated for each testing user. In the Record Details view, see the Trail Evaluation field for each record. It will have a value even for trail record of the OMEGACATESTDEV02 user and empty for the last OMEGACATESTDBA01. The policy name will be "EVL Developer Access". The policy Result will be TRUE.

### 2.2.4 Access Control for DBA

Rationale:
The "EVL DBA Access" policy establishes a secure logon channel for the DBA User OMEGACATESTDBA01. Policy is created with User Appliance of type "Users Apply" for user OMEGACATESTDBA01 only.

In Omega Core Audit open the Access Control policy "EVL DBA Access". Open its rule "DBA Access". Activate the two Operand Conditions of Session User and Client Host. For the later set the right "Operand 1" value instead of the provided <DOMAIN\HOST>. Activate the rule "DBA Access". Activate the policy "EVL DBA Access".

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.

In Omega Core Audit, search the unified trail. You will see an Access Control trail record generated for each testing user. In the Record Details view, see the Trail Evaluation field for each record. It will have a value even for the trail record of the OMEGACATESTDBA01. The policy name will be "EVL DBA Access". The policy Result will be TRUE.

### 2.2.5 Access Control for Oracle Connections

Rationale:
The "EVL Oracle Internals" policy establishes a secure logon channel for the Oracle own schemas SYS, SYSMAN and DBSNMP. Policy is created with User Appliance of type "Users Apply" for users SYS, SYSMAN and DBSNMP.

In Omega Core Audit open the Access Control policy "EVL Oracle Internals". Open its only rule "Oracle Connections". Activate the two Operand Conditions of Session User and Client Host. For the later set the right "Operand 1" value instead of the provided <DB-SRV>. Activate the rule "Oracle Connections". Activate the policy "EVL Oracle Internals".

This is not tested with the Benchmark software!
At this point, to test the policy above you can:

1. Wait for the Oracle SYS run jobs to execute. In a normal environment, you will have active job[s], even at a one minute interval.
2. Simulate yourself by manually opening a SYS/SYSMAN session from a SQL terminal, or best a SYS session as SYSDBA (OS authentication) on the DB server.

In Omega Core Audit, search the unified trail for Username equal to SYS only. You will see that in the Access Control Trail records generated by SYS, Record Details view, the Trail Evaluation field will have a value and is not empty as before this policy appliance. The policy name will be "EVL Oracle Internals". The policy Result will be TRUE.

### 2.2.6 Tuning the Access Control

Rationale:
Optimize Access Control for auditing knowledgeably and performance.

Having all the Access Control policies above with an Audit Option of "On Success/Failure" might not be a good idea for the Application Access policy. For example, behind the Application Schema Owner Oracle account may be hundreds of application users and new sessions might be (application's developer choice) created at every form open, or refresh, in case of web-design. Having the policy "EVL Application Access" on such a configuration could generate hundreds if not thousands of repetitive log entries per minute, so it would be logically to have the trail log only when the policy is not satisfied.

On the Access Control policy "EVL Application Access", set the Audit Option to "On Failure".

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.

In Omega Core Audit, search the unified trail. You will notice that Access Control trail records will be created for all users, except OMEGACATESTAPP01.

### 2.2.7 Enforcing the Access Control

Rationale:
Enforce Access Control on the database by rejecting non-complying logons.

Until now we have used the Access Control module in its default Silent Mode. This means the logon actions were allowed to continue whatever the compliance evaluation (Policy Result TRUE/FALSE) was.

To test the protective capabilities of the Access Control module, into the Omega Core Audit software, System Components form, Access Control tab, uncheck the Silent Checkbox and press the Set button to set the changed value. Also change the "Developer 02 Access" rule of the "Developer Access" and wrongly set the Client Host Operand Condition's value, so that rule evaluates FALSE.

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.
You will notice the logon failure "ORA-20010: Access Control Policy non-compliance!" only for the OMEGACATESTDEV02 user. The OMEGACATESTDEV02 logon action has been rejected!

In Omega Core Audit, search the unified trail. You will notice the same error code and message in the same unified trail fields Return Code and Return Message for the OMEGACATESTDEV02 user. The Trail Evaluation field will be "EVL Developer Access". The policy Result will be FALSE.

**Note**
If you will continue the testing with Silent Mode unset, make sure to have rightly ensured the logon of the four testing users, so that they continue perform other module's commands.
The same is required for the OMEGACAADM (Omega Core Audit pre-configured Administrator) user, needed for operating on the Omega Core Audit Application.

# 3 Evaluating the Standard Audit

This chapter is a walkthrough on the Standard Audit module implementation administered through the Omega Core Audit Application and benchmarked via the Omega Core Audit Benchmark software.

## 3.1 Prerequisites

- The database parameter AUDIT_TRAIL has been set to DB_EXTENDED and DB restarted (change effective).
- The Standard Audit module's Map option must have been set. See in System Components form, tab DB Audit Trails Purge, Group "Std. Aud Map", checkbox Map must be checked. This is not the default setting after the Install!
- The DB Audit Trails Purge job has been stopped. We will immediately retrieve the logs by the manually invoking the DB Audit Trails Purge job.
- Drop any Oracle Default user-wide audit settings, as advised in Deployment Guide, Appendix Utility Scripts, Topic Oracle Statement and Objects Audits, part ORACLE STATEMENT AUDITS for user-wide Statement Audits. You can re-enable them later through the "Oracle Default Audits" policy.

## 3.2 Benchmark Testing

### 3.2.1 Initialization

Rationale:
There is yet no Active Policy. The install provided "Oracle Default Audits" policy is Inactive.

In the Omega Core Audit Benchmark software, Testing Options group, check only the DML Checkbox. Check all the five DML commands. Check all the four Users.

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.
In the Omega Core Audit manually invoke the DB Audit Trails Purge procedure.

In Omega Core Audit, search the unified trail. There will be no Standard Audit records (Policy Type equal to Standard Audit), because no policy's rule has been activated yet, either on user statements or objects.

### 3.2.2 Standard Audit for Developer Users

Rationale:
The "EVL Developer Audit" policy audits statements and system privileges from Developer Users. Policy is created with a Policy Type of "Statement [Priv.]".

In Omega Core Audit open the Standard Audit policy "EVL Developer Audit". Activate the first four rules, namely INSERT/SELECT/DELETE/UPDATE TABLE for the first Developer OMEGACATESTDEV01. Activate the policy "EVL Developer Audit".

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.
In the Omega Core Audit manually invoke the DB Audit Trails Purge procedure.

In Omega Core Audit, search the unified trail. Standard Audit trails have been created only for the OMEGACATESTDEV01 user. In the Record Details view, see the Trail Evaluation field. The policy name will be "EVL Developer Audit". The policy Result will be TRUE.

Activate the second four rules, namely INSERT/SELECT/DELETE/UPDATE TABLE for the second Developer OMEGACATESTDEV02.

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.
In the Omega Core Audit manually invoke the DB Audit Trails Purge procedure.

In Omega Core Audit, search the unified trail. Standard Audit trails have been created even for the OMEGACATESTDEV02. In the Record Details view, see the Trail Evaluation field. The policy name will be "EVL Developer Audit". The policy Result will be TRUE.

### 3.2.3 Standard Audit for Application Objects

Rationale:
The "EVL App Obj Audit" policy audits operations on objects. Policy is created with a Policy Type of "Object".

In Omega Core Audit open the Standard Audit policy "EVL App Obj Audit". Activate its two rules, namely DELETE/UPDATE on the EMP table owned by OMEGACATESTAPP01. Activate the policy "EVL App Obj Audit".

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.
In the Omega Core Audit manually invoke the DB Audit Trails Purge procedure.

In Omega Core Audit, search the unified trail. Standard Audit trails have been created even for the OMEGACATESTAPP01 and OMEGACATESTDBA01 users, but only for their DELETEs and UPDATEs on EMP. In the Record Details view, see the Trail Evaluation field. The policy name will be "EVL App Obj Audit". The policy Result will be TRUE.

### 3.2.4 Standard Audit for DBA Users

Rationale:
The "EVL DBA Audit" policy audits statements and system privileges from DBA Users. Policy is created with a Policy Type of "Statement [Priv.]".

In Omega Core Audit open the Standard Audit policy "EVL DBA Audit". Activate the first three rules, namely the INSERT ANY TABLE/DELETE ANY TABLE /UPDATE ANY TABLE for the OMEGACATESTDBA01 user. Activate the policy "EVL DBA Audit".

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.
In the Omega Core Audit manually invoke the DB Audit Trails Purge procedure.

In Omega Core Audit, search the unified trail. Standard Audit trails have been created even for INSERT on EMP for the OMEGACATESTDBA01 user. In the Record Details view, see the Trail Evaluation field. The policy name will be "EVL DBA Audit". The policy Result will be TRUE.

In the following we will evaluate Standard Audit of certain important security related DDLs, namely Grant and Revokes commands for granting system privileges, roles and object privileges to grantees.

In the Omega Core Audit Benchmark software, Testing Options group, uncheck the DML Checkbox and check only the Security Checkbox. Check all the six Security Commands and in the Users grid check only the OMEGACATESTDBA01 user.

Activate the second two rules, namely the SYSTEM GRANT and GRANT ANY OBJECT PRIVILEGE for the OMEGACATESTDBA01 user.

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.
In the Omega Core Audit manually invoke the DB Audit Trails Purge procedure.

In Omega Core Audit, search the unified trail. Standard Audit trails have been created even for the Grants and Revokes performed by the OMEGACATESTDBA01 user. In the Record Details view, see the Trail Evaluation field. The policy name will be "EVL DBA Audit". The policy Result will be TRUE.

### 3.2.5 Tuning the Standard Audit

Rationale:
Optimize Standard Audit for auditing knowledgeably and performance.

As you have noticed, there is no Audit Option configuration into the Standard Audit policy. Meanwhile policies are of two types, according to Oracle user statements or object they can audit with their rules.

Actions performed on the database by Developers and DBA Users are expected to be infrequent and insignificant comparing to the whole system work. But these actions are exercised by privileged users and as such are worthy for audit. User-statement audits are activated on such type of accounts and Standard Audit policies of type Statement [Priv.] do implement them.

For example, auditing the OMEGACATESTDEV01 Developer user for DELETE TABLE will audit him not only for delete of OMEGACATESTAPP01.EMP, but even for OMEGACATESTAPP01.DEPT or any other schema/table. Users granted privilege of kind ANY (DELETE ANY TABLE) should be audited for ANY statements, like our DBA user OMEGACATESTDBA01.

As for auditing actions launched by the Application Owner itself, using exactly the method above would not be a good idea, considering the case that behind the Application Schema Owner Oracle account may be hundreds of application users and new sessions might be (application's developer choice) created at every form open, or refresh, in case of web-design. Such a configuration could generate hundreds if not thousands of repetitive log entries per minute, so it would be logically to either reduce the user-statements audits, or better, to implement Standard Audit policies of type "Object" on the objects of importance, as we have done with the policy ‘‘Application Objects" for DELETE and UPDATE on the application owner OMEGACATESTAPP01 table's EMP, but not for SELECT.

# 4 Evaluating the Real-Time Protection DDL

This chapter is a walkthrough on Real-Time Protection DDL implementation administered through the Omega Core Audit Application and benchmarked via the Omega Core Audit Benchmark software.

## 4.1 Prerequisites

- The Real-Time Protection DDL Module has been activated

## 4.2 Benchmark Testing

### 4.2.1 Initialization

Rationale:
Real-Time Protection DDL Module is activated and there is yet no Active Policy.

In the Omega Core Audit Benchmark software, Testing Options group, check only the DDL Checkbox. Check all the four DDL commands. Check all the four Users.

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.

In Omega Core Audit, search the unified trail. There will be no Real-Time Protection DDL records (Policy Type equal to RTP-DDL), because no policy has been activated yet.

### 4.2.2 Real-Time Protection DDL for Application Objects

Rationale:
The "EVL Application DDls" policy establishes a secure channel for DDLs performed by Developers on the Application Owner schema objects. Policy is created with User Appliance of type "All Users".

In Omega Core Audit open the Real-Time Protection DDL policy "EVL Application DDls". Open its rule "Developer 01 DDL". Activate the two Operand Conditions of Session User and Client Host. For the later set the right "Operand 1" value instead of the provided <DOMAIN\HOST>. Activate the rule "Developer 01 DDL". Activate the policy "EVL Application DDls".

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.

In Omega Core Audit, search the unified trail. You will see Real-Time Protection DDL trail records generated for each testing user. In the Record Details view, see the Trail Evaluation field for each record. The policy name will be "EVL Application DDls". The policy Result will be TRUE only for the OMEGACATESTDEV01 user and FALSE for all three other users.

Open the rule "Developer 02 DDL". Activate the two Operand Conditions of Session User and Client Host. For the later set the right "Operand 1" value instead of the provided <DOMAIN\HOST>. Activate the rule "Developer 02 DDL".

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.

In Omega Core Audit, search the unified trail. You will see Real-Time Protection DDL trail records generated for each testing user. In the Record Details view, see the Trail Evaluation field for each record. The policy name will be "EVL Application DDls". The policy Result will be TRUE even for the OMEGACATESTDEV02.

At this stage, only the OMEGACATESTAPP01 (Schema Owner Itself) and OMEGACATESTDBA01's (the DBA) records show evaluate FALSE of the policy, which means are not authorized to perform DDLs on the Application Objects.

### 4.2.3 Real-Time Protection DDL for Security Privileges

Rationale:
The "EVL Security Privileges" policy establishes a secure channel for the Grant and Revoke Security (DDL) commands performed on the database. Policy is created with User Appliance of type "All Users".

In the following we will evaluate Real-Time Protection DDL of certain important security related DDLs, namely Grant and Revokes commands for granting system privileges, roles and object privileges to grantees.

In the Omega Core Audit Benchmark software, Testing Options group, uncheck the DDL Checkbox and check only the Security Checkbox. Check all the six Security Commands and in the Users grid check only the OMEGACATESTDBA01 user.

In Omega Core Audit open the Real-Time Protection DDL policy "EVL Security Privileges". Open its rule "DBA Security". Activate the two Operand Conditions of Session User and Client Host. For the later set the right "Operand 1" value instead of the provided <DOMAIN\HOST>. Activate the rule "DBA Security". Activate the policy "EVL Security Privileges".

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.

In Omega Core Audit, search the unified trail. You will see Real-Time Protection DDL trail records generated for the OMEGACATESTDBA01 user. In the Record Details view, see the Trail Evaluation field for each record. The policy name will be "EVL Security Privileges". The policy Result will be TRUE.

### 4.2.4 Tuning the Real-Time Protection DDL

Rationale:
Optimize Real-Time Protection DDL for auditing knowledgeably and performance.

The Real-Time Protection DDL generates insignificant load to the system, considering that DDL (Data definition language) commands are very rare comparing to the rest of system actions. Due to the importance of the subject, such as structural change is, detailed audit is advised, like existing DDL Body and SQL given. Although full DDL audit can be performed, it is recommended to narrow the scope of the auditing to the areas of interest.

### 4.2.5 Enforcing the Real-Time Protection DDL

Rationale:
Enforce Real-Time Protection DDL on the database by rejecting non-complying DDLs.

Until now we have used the Real-Time Protection DDL Policies in their default Silent Deny Mode. This means the DDL actions were allowed to continue whatever the compliance evaluation was.

To test the protective capabilities of the Real-Time Protection module, in the Omega Core Audit software, open the Real-Time Protection DDL policy "EVL Application DDls". Uncheck the Silent Deny Checkbox and press the Save button to save the policy.

In the Omega Core Audit Benchmark software, Testing Options group, uncheck the Security Checkbox and re-check only the DDL Checkbox. Check all the four DDL Commands. Check all the four users.

Remember that in the RTP DDL Policy "EVL Application DDls", we have authorized only the two Developers to perform DDLs on the Application Schema Owner, through two respective RTP DDL rules.

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.
You will notice DDL failure "ORA-20010: RTP DDL Policy: EVL Application DDls violation!" for the OMEGACATESTAPP01 and OMEGACATESTDBA01 users. The Application Owner's itself and the DBAs DDL actions have been rejected.

In Omega Core Audit, search the unified trail. You will see Real-Time Protection DDL trail records generated for the OMEGACATESTDBA01 user. In the Record Details view, see the Trail Evaluation field for each record. The policy name will be "EVL Security Privileges". The policy Result will be TRUE for OMEGACATESTDEV01 and OMEGACATESTDEV02 and FALSE for OMEGACATESTAPP01 and OMEGACATESTDBA01.

You can do the same (disable Silent Deny) with the other policy.

# 5 Evaluating the Real-Time Protection DML

This chapter is a walkthrough on Real-Time Protection DML implementation administered through the Omega Core Audit Application and benchmarked via the Omega Core Audit Benchmark software.

## 5.1 Prerequisites

- The Real-Time Protection DML module's Map option must have been set. See in System Components form, tab DB Audit Trails Purge, Group "RTP DML Map", checkbox Map must be checked. This is not the default setting after the Install! On the same Group "RTP DML Map", check also that "Rtn." checkbox is checked, this is default in install.
- The DB Audit Trails Purge job has been stopped. We will immediately retrieve the logs by the manually invoking the DB Audit Trails Purge job.

## 5.2 Benchmark Testing

### 5.2.1 Initialization

Rationale:
There is yet no Active Policy.

In the Omega Core Audit Benchmark software, Testing Options group, check only the DML Checkbox. Check all the five DML commands. Check all the four Users.

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.
In the Omega Core Audit manually invoke the DB Audit Trails Purge procedure.

In Omega Core Audit, search the unified trail. There will be no Real-Time Protection DML records (Policy Type equal to RTP-DML), because no policy's rule has been activated yet.

### 5.2.2 Real-Time Protection DML for Application Objects

Rationale:
The "EVL Application DMLs" policy establishes a secure channel for DMLs performed on the Application Owner's table EMP. Policy is created with User Appliance of type "All Users".

In Omega Core Audit open the Real-Time Protection DML policy "EVL Application DMLs". Open its rule "EMP Data". When opening the rule, you will get the error: "Oracle Audit policy Pot found for rule". This is because the policy's rule has not yet been fully created; its Oracle FGA policy part is yet non-existing.

Complete the missing parts of the RTP DML Rule "EMP Data", namely: check all the four SEL, INS, DEL, UPD Statements, set the Audit Trail to DB_EXTENDED and Column Options to ANY_COLUMNS. Do not check any object columns from those listed on the right. In the Rule Authorization group below, radio Group Authorization type, Radio box "No Condition" remains checked (default). Press the SAVE button to save changes made to the "EMP Data" rule! Activate the rule "EMP Data". Activate the policy "EVL Application DMLs".

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.

In the Omega Core Audit manually invoke the DB Audit Trails Purge procedure.

In Omega Core Audit, search the unified trail. Real-Time Protection DML trails have been created for all testing users and all their actions. In the Record Details view, see the Trail Evaluation field. The policy name will be "EVL Application DMLs". The policy Result will be TRUE. The Audit event has been triggered for all testing users and actions, the DMLs in Benchmark have been successful only because the Rule EMP Data is in Silent Deny mode (default on RTP DML Rule create).

In Omega Core Audit, change the Real-Time Protection DML rule "EMP Data" Rule. Unselect the Statements options INSERT, UPDATE and DELETE, leaving only the SELECT. Also in Omega Core Audit Benchmark DML commands list, uncheck all DMLs, except the SELECTSs (DML2 and DML5)!

We will keep it this way the rest of this evaluation only for the sake of simplicity, to have fewer records in the unified trail!

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.
In the Omega Core Audit manually invoke the DB Audit Trails Purge procedure.

In Omega Core Audit, search the unified trail. There will be again Real-Time Protection DML trails created for all users, but only for the SELECT action.

Up to this point now, the Real-Time Protection DML Rule looks similar to the Standard Audit Object Rule. However, some extra features that you might have already noted are the ones that make the difference, like: the protective capabilities, context based authorization (Authorization type of Rule Conditions), audit and protection triggering on columns returned, column conditions (row based), row value conditions (SALARY>3000) and the ability to decide completion of SQL Bind and Text fields, latterly discussed.

In the following topics we will explore the advanced capabilities of the Real-Time Protection DML Policy.

### 5.2.3 Real-Time Protection DML - Rule Conditions Authorization

Rationale:
Using Real-Time Protection DML with Rule Authorization Type of Rule Conditions to achieve user-environment context evaluation, which means evaluating Rule by its Conditions (as for the rules in Access Control and Real-Time Protection DDL).

In Omega Core Audit change the "EMP Data" Rule. In the Rule Authorization group below, radio Group Authorization type, check the "Rule Conditions" Radio box. The Rule Conditions tab will open below. Set the Condition Evaluation combo box from "None" to "Any True"! Press the SAVE button to save changes made to the "EMP Data" rule!

Activate the two Operand Conditions of Session User and Client Host. For the later set the right "Operand 1" value instead of the provided <DOMAIN\HOST>.

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.
In the Omega Core Audit manually invoke the DB Audit Trails Purge procedure.

In Omega Core Audit, search the unified trail. There will be Real-Time Protection DML trails created for all users, except for the Application Owner OMEGACATESTAPP01. This is because with the configuration of the DML Rule above, we have created a secure DML channel for the SELECTs on EMP performed by the Application Owner account (Session User) and coming from the Client Host. We are not requiring an audit event in this case, but in all its violations.

### 5.2.4 Real-Time Protection DML - Column Condition (row-based)

Rationale:
The use of Real-Time Protection DML with Rule Authorization Type of Column Condition achieves application context evaluation by setting conditions on application table's column values (row-based).

At this point (for this topic and for the next), you are advised to take a look at the content of the EMP table. In your IDE of choice, run the following SQL:

```
SELECT * FROM
OMEGACATESTAPP01.V_EMP
ORDER BY EMP_ID
```

That will show the employees and some features like department and (important!) the Salary.

Also in Omega Core Audit Benchmark examine the DML commands DML2 and DML5, are respectively as:

```
DML2:   select first_name, last_name from OMEGACATESTAPP01.emp where dept_id = 2
DML5:   select first_name, last_name, dept_id, salary from OMEGACATESTAPP01.emp where dept_id = 3
```

In Omega Core Audit, change the "EMP Data" rule. In the Rule Authorization group, radio Group Authorization type, check the "Column Condition" Radio box. The Column Condition tab will open below. Set the Operation Code to > and Operand 1 to 3000. Drag and drop the SALARY column (found in the Object Columns checklist) to the Authorization Condition memo below. The condition SALARY>3000 will be set. Save the "EMP Data" Rule.

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.
In the Omega Core Audit manually invoke the DB Audit Trails Purge procedure.

In Omega Core Audit, search the unified trail. There will be Real-Time Protection DML trails created for all users (even for Application Owner OMEGACATESTAPP01), but only for the DML5 and not DML2. This because in the DML Rule above, we are requesting an audit event for all SELECTS of rows where SALARY>3000; in DML2, the WHERE condition DEPT_ID=2 retrieves only employees of the Operations Department (ID=2), whose Salary is less than 3000, thus no audit event is triggered. In DML5 instead, the WHERE condition DEPT_ID=3 retrieve the employee of the Finance Department (ID=3), whose Salary is more than 3000.

### 5.2.5 Real-Time Protection DML - Column-based

Rationale:
The use of Real-Time Protection DML with Column Options achieves application context evaluation by application table's column access.

In the Omega Core Audit change again the "EMP Data" Rule. In the Rule Authorization group, radio Group Authorization type, check the "No Condition" Radio box. This is done for the sake of simplicity, since the choice of the columns (and their effect) in the RTP DML Rule is independent of the Authorization Type chosen! In the Object Columns checklist, check the FIRST_NAME, LAST_NAME and SALARY columns. Change the Column Options from ANY_COLUMN (so far) to ALL_COLUMNS. Save the "EMP Data" Rule.

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.
In the Omega Core Audit manually invoke the DB Audit Trails Purge procedure.

In Omega Core Audit, search the unified trail. There will be Real-Time Protection DML trails created for all users, but only for the DML5 and not for DML2. This is because although FIRST_NAME and LAST_NAME columns are queried in both DML2 and DML5, the SALARY column is missing in queried only in DML5.

### 5.2.6 Tuning the Real-Time Protection DML

Rationale:
Optimize Real-Time Protection DML for auditing knowledgeably and performance.

As you have noticed, there is no Audit Option configuration into the Standard Audit policy.

The Real-Time Protection DML mechanism is mostly advised to be used for important objects. Use it mostly to audit (and optionally protect by rejection) privileged accounts actions on such objects and every divergence from normal behavior, implemented in DML Rule.

Used the way above, the Real-Time Protection DML will generate insignificant load to the system.

In general, tuning the Real-Time Protection DML assembles Tuning Requirements from all other three modules, as the Omega Core Audit internals are built such.

### 5.2.7 Enforcing the Real-Time Protection DML

Rationale:
Enforce Real-Time Protection DML on the application objects by rejecting non-complying DMLs.

Until now we have used the Real-Time Protection DML Rules in their default Silent Deny Mode. This means the DML actions were allowed to continue even when the audit event is triggered.

To test the protective capabilities of the Real-Time Protection DML rule, into the Omega Core Audit software, change again the DML Rule "EMP Data". In the Rule Authorization group below, radio Group Authorization type, check the "Rule Conditions" Radio box. The Rule Conditions tab will open below. Set the Condition Evaluation combo box from "None" to "Any True"! Uncheck all the checked Object Columns and set the Column Options back again to ANY_COLUMNS. Uncheck the Silent Deny Checkbox! Press the Save button to save the "EMP Data" Rule.

Press the Run button in Omega Core Audit Benchmark and wait until it finishes.
You will notice that only the DMLs of Application Owner OMEGACATESTAPP01 have been successful, while for all others (the two Developers and the DBA) you will notice the error "ORA-20010: RTP DML Rule violation Id: [Rule_ Id] Rule Name: EMP Data!". The SELECT DML actions on EMP have been rejected for all users other then the Application Schema Owner.

In the Omega Core Audit manually invoke the DB Audit Trails Purge procedure.

In Omega Core Audit, search the unified trail. There will be Real-Time Protection DML trails for the OMEGACATESTDEV01, OMEGACATESTDEV02 and OMEGACATESTDBA01 users. Notice the error message "RTP DML Policy Rule: EMP Data violation!".

# 6 Summary and Conclusions

The tests described so far in this document represent only a small view of the Omega Core Audit capabilities. The benchmark testing has been performed with the Omega Core Audit Benchmark, but your final tests should be performed in test environments as similar as possible to your Live Database.

You are encouraged to try other combinations of audit/protection settings in Omega Core Audit. Do the same for the options into the Omega Core Audit Benchmark.

Mind the differences of audit and protection features in each module.

It would be logical that some knowledge from the Omega User's Guide is required, may be not for exactly the above walkthrough guide, but surely for advanced testing options you may perform, or furthermore in your test-simulated environment and finally your Live Database.

# 7 Support

For technical support please use the support area on our site www.dataplus-al.com/support. Here you can find product documentation, knowledge base, raise support service requests and more.

Browse our site www.dataplus-al.com for updated information.

You can also send an e-mail to support@dataplus-al.com.

Support and upgrades are offered to registered and commercials users only. However, just by registering for free you will have free and unlimited access to latest software packages download, documentations and utilities.

We do commit to offer support to evaluation users too and also arrange remote trainings, demos and implementations on their systems.

DATAPLUS
Tirana, Albania
Street Address: Bul. Zog I, P. "Edicom", 8F.

| | |
|---|---|
| E-Mail: | info@dataplus-al.com |
| Cel: | +355 68 2061664 |
| Tel: | +355 00000000 |

# 8 ANNEXES

## 8.1 ANNEX 1. Evaluation Policies

Below are the evaluation policies, as originally created directly on the repository by the provided .sql script.

### 8.1.1 Access Control

| **Policy** | **Policy Name** | **Description** | **Audit Option** | **User Appliance** | **Rule Eval.** |
|---|---|---|---|---|---|
| 1. | EVL Application Access | EVL Application Access | On Success/Failure | Users Apply | Any True |
| **Rules** | **Rule Name** | **Rule Description** | **Condition Eval.** | | |
| 1. | App. Owner 01 Access | App. Owner 01 Access | All True | | |
| **Conditions** | **Factor** | **Condition Evaluation** | **Operation Code** | **Operand 1** | **Operand 2** |
| 1. | Session User | Operand | = | OMEGACATESTAPP01 | |
| 1. | Client Host | Operand | = | <DOMAIN/HOST> | |

| **Policy** | **Policy Name** | **Description** | **Audit Option** | **User Appliance** | **Rule Eval.** |
|---|---|---|---|---|---|
| 1. | EVL Developer Access | EVL Developer Access | On Success/Failure | Users Apply | Any True |
| **Rules** | **Rule Name** | **Rule Description** | **Condition Eval.** | | |
| 1. | Developer 01 Access | Developer 01 Access | All True | | |
| **Conditions** | **Factor** | **Condition Evaluation** | **Operation Code** | **Operand 1** | **Operand 2** |
| 1. | Session User | Operand | = | OMEGACATESTDEV01 | |
| 2. | Client Host | Operand | = | <DOMAIN/HOST> | |
| **Rules** | **Rule Name** | **Rule Description** | **Condition Eval.** | | |
| 2. | Developer 02 Access | Developer 02 Access | All True | | |
| **Conditions** | **Factor** | **Condition Evaluation** | **Operation Code** | **Operand 1** | **Operand 2** |
| 1. | Session User | Operand | = | OMEGACATESTDEV02 | |
| 2. | Client Host | Operand | = | <DOMAIN/HOST> | |

| **Policy** | **Policy Name** | **Description** | **Audit Option** | **User Appliance** | **Rule Eval.** |
|---|---|---|---|---|---|
| 1. | EVL DBA Access | EVL DBA Access | On Success/Failure | Users Apply | Any True |
| **Rules** | **Rule Name** | **Rule Description** | **Condition Eval.** | | |
| 1. | DBA 01 Access | DBA 01 Access | All True | | |
| **Conditions** | **Factor** | **Condition Evaluation** | **Operation Code** | **Operand 1** | **Operand 2** |
| 1. | Session User | Operand | = | OMEGACATESTDBA01 | |
| 2. | Client Host | Operand | = | <DOMAIN/HOST> | |

| **Policy** | **Policy Name** | **Description** | **Audit Option** | **User Appliance** | **Rule Eval.** |
|---|---|---|---|---|---|
| 1. | EVL Oracle Internals | EVL Oracle Internals | On Success/Failure | Users Apply | Any True |
| **Rule** | **Rule Name** | **Rule Description** | **Condition Eval.** | | |
| 1. | Oracle Connections | Oracle Connections | All True | | |
| **Condition** | **Factor** | **Condition Evaluation** | **Operation Code** | **Operand 1** | **Operand 2** |
| 2. | Client Host | Operand | = | <DB-SRV> | |

### 8.1.2 Standard Audit

| **Policy** | **Policy Name** | **Description** | **Type** |
|---|---|---|---|
| 1. | Developer Audit | Developer Audit | Statement [Priv.] |
| **Rule** | **Statement** | **Username** | **Success/Failure** |
| 1. | DELETE TABLE | OMEGACATESTDEV01 | Success/Failure |
| 2. | INSERT TABLE | OMEGACATESTDEV01 | Success/Failure |
| 3. | SELECT TABLE | OMEGACATESTDEV01 | Success/Failure |
| 4. | UPDATE TABLE | OMEGACATESTDEV01 | Success/Failure |
| 5. | DELETE TABLE | OMEGACATESTDEV02 | Success/Failure |
| 6. | INSERT TABLE | OMEGACATESTDEV02 | Success/Failure |
| 7. | SELECT TABLE | OMEGACATESTDEV02 | Success/Failure |
| 8. | UPDATE TABLE | OMEGACATESTDEV02 | Success/Failure |

| **Policy** | **Policy Name** | **Description** | **Type** | | |
|---|---|---|---|---|---|
| 1. | App Obj Audit | App Obj Audit | Object | | |
| **Rule** | **Object Owner** | **Object Type** | **Object Name** | **Audit Operation** | **Success/Failure** |
| 1. | OMEGACATESTAPP01 | TABLE | EMP | DELETE | Success/Failure |
| 2. | OMEGACATESTAPP01 | TABLE | EMP | UPDATE | Success/Failure |

| **Policy** | **Policy Name** | **Description** | **Type** |
|---|---|---|---|
| 1. | DBA Audit | DBA Audit | Statement [Priv.] |
| **Rule** | **Statement** | **Username** | **Success/Failure** |
| 1. | DELETE ANY TABLE | OMEGACATESTDBA01 | Success/Failure |
| 2. | INSERT ANY TABLE | OMEGACATESTDBA01 | Success/Failure |
| 3. | SELECT ANY TABLE | OMEGACATESTDBA01 | Success/Failure |
| 4. | UPDATE ANY TABLE | OMEGACATESTDBA01 | Success/Failure |

### 8.1.3 Real-Time Protection DDL

| **Policy** | **Policy Name** | **Description** | **Audit Option** | **User Appliance** | **Rule Eval.** |
|---|---|---|---|---|---|
| 1. | EVL Application DDls | EVL Application DDls | On Success/Failure | All Users | Any True |
| **Rule** | **Rule Name** | **Rule Description** | **Condition Eval.** | | |
| 1. | Developer 01 DDL | Developer 01 DDL | All True | | |
| **Condition** | **Factor** | **Condition Evaluation** | **Operation Code** | **Operand 1** | **Operand 2** |
| 1. | Session User | Operand | = | OMEGACATESTDEV01 | |
| 2. | Client Host | Operand | = | <DOMAIN/HOST> | |
| **Rule** | **Rule Name** | **Rule Description** | **Condition Eval.** | | |
| 2. | Developer 02 DDL | Developer 02 DDL | All True | | |
| **Condition** | **Factor** | **Condition Evaluation** | **Operation Code** | **Operand 1** | **Operand 2** |
| 1. | Session User | Operand | = | OMEGACATESTDEV02 | |
| 2. | Client Host | Operand | = | <DOMAIN/HOST> | |

| **Policy** | **Policy Name** | **Description** | **Audit Option** | **User Appliance** | **Rule Eval.** |
|---|---|---|---|---|---|
| 1. | Security Privileges | Security Privileges | On Success/Failure | All Users | Any True |
| **Rule** | **Rule Name** | **Rule Description** | **Condition Eval.** | | |
| 1. | DBA Security | DBA Security | All True | | |
| **Condition** | **Factor** | **Condition Evaluation** | **Operation Code** | **Operand 1** | **Operand 2** |
| 1. | Session User | Operand | = | OMEGACATESTDBA01 | |
| 2. | Client Host | Operand | = | <DOMAIN/HOST> | |

### 8.1.4 Real-Time Protection DML

| **Policy** | **Policy Name** | **Description** | **User Appliance** | | |
|---|---|---|---|---|---|
| 1. | Application Objects | Application Objects | All Users | | |
| **Rule** | **Rule Name** | **Rule Description** | **Authorization Type** | **Condition Eval.** | |
| 1. | EMP Data | EMP Data | Rule Conditions | Any True | |
| **Condition** | **Factor** | **Condition Evaluation** | **Operation Code** | **Operand 1** | **Operand 2** |
| 1. | Session User | Operand | <> | OMEGACATESTAPP01 | |
| 2. | Client Host | Operand | <> | <DOMAIN/HOST> | |