accenture
High performance. Delivered.

Accenture Enkitec Group

ORACLE TECHNOLOGY NETWORK LatinAmerica

Oracle Data Redaction

Presented by:

Alex Zaballa, Oracle DBA 

Alex Zaballa

ORACLE ACE Director

ORAWORLD

147 and counting…

http://alexzaballa.blogspot.com/

@alexzaballa

https://www.linkedin.com/in/alexzaballa

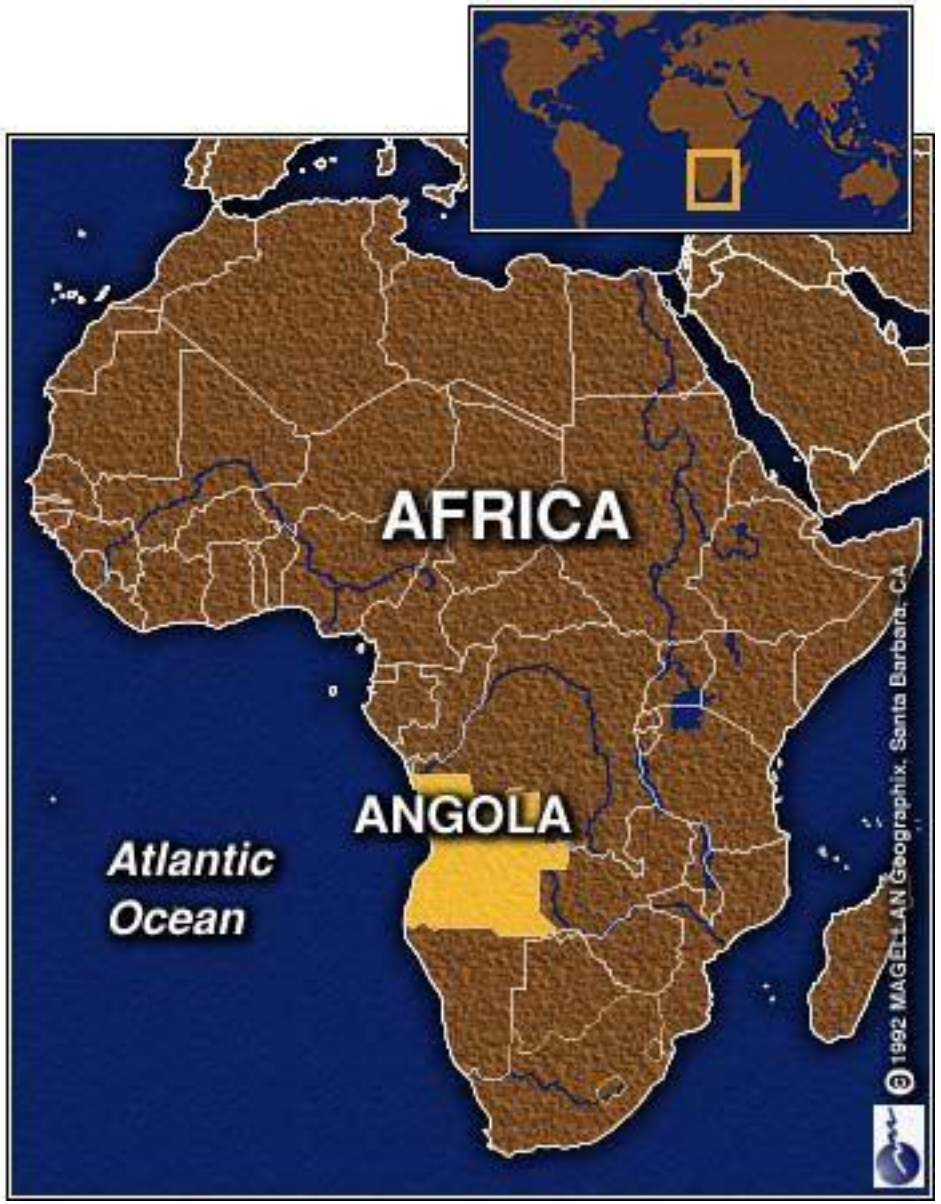
GUOB

Ministério das Finanças de Angola:

Março de 2007 até Março de 2008
Março de 2009 até Março de 2015

Sicredi:

Março de 2008 até Março de 2009



ORACLE
TECHNOLOGY NETWORK
LatinAmerica

accenture

Accenture
Enkitec Group

High performance. Delivered.

ORACLE TECHNOLOGY NETWORK
LatinAmerica

Oracle Specializations

- Oracle Database
- Oracle Exadata
- Oracle GoldenGate
- Oracle Data Integrator
- Oracle Data Warehouse
- Oracle Real Application Clusters
- Oracle Performance Tuning
- Oracle Database Security

Global systems integrator
focused on the Oracle Database
& Engineered Systems platform

Worldwide leader in Exadata
implementations (600+)

ORACLE TECHNOLOGY NETWORK
LatinAmerica

ORACLE ACE PROGRAM

http://www.oracle.com/technetwork/community/oracle-ace/index.html

Oracle Community Experts and Advocates

What is an Ace? +

ACE Levels +

Find an ACE +

500+

Technical experts and evangelists are active in this global network.

ORACLE TECHNOLOGY NETWORK
LatinAmerica

Neto, Antonio Jose Rodrigues
Database Management & Performance
Brasil

Wagner Bianchi
MySQL
Brasil

Marcus Vinicius Miguel Pedro
Database Management & Performance
Brasil

Rodrigo Mufalani
Database Management & Performance
Brasil

Ricardo Portilho Proni
Database Management & Performance
Brasil

Eduardo Legatti
Database Management & Performance
Brasil

Fabio Prado
Database Management & Performance
Brasil

David Siqueira
Database Management & Performance
Brasil

Alexandre Borges
Solaris
Brasil

Alex Zaballa
Database Management & Performance
Brasil

Rodrigo Almeida
Database Management & Performance
Brasil

Carlos H. Y. Furushima
Database Management & Performance
Brasil

Rodrigo Radtke de Souza
Business Intelligence
Brazil

Ricardo Giampaoli
Business Intelligence
Brazil

Eduardo Schurtz
Applications & Apps Technology
Brasil

Felipe Idalgo
Business Intelligence
Brasil

Uanderson Carvalho
Middleware & SOA
Brasil

ORACLE TECHNOLOGY NETWORK LatinAmerica

ORACLE | Oracle Community Directory | Oracle Community FAQ

ORACLE TECHNOLOGY NETWORK

GO

All Places > Other Languages > Portuguese

Portuguese

Overview Content People Subspaces

Log in to follow, share, and participate in this community.

SPACE TREE

- General Database Discussions (Portuguese)
- SQL and PL/SQL (Portuguese)
- OTN América Latina Tour 2015 View 12 sub-spaces
- OpenWorld & JavaOne Latin America 2015

https://community.oracle.com/community/other-languages/portuguese

accenture
High performance. Delivered.

Accenture Enkitec Group

ORACLE TECHNOLOGY NETWORK LatinAmerica

Oracle Data Redaction

Data Redaction

- One of the new features introduced in Oracle Database 12c
- Part of the Advanced Security option
- Enables the protection of data shown to the user in real time, without requiring changes to the application

Data Redaction

- This new feature has been backported to Oracle Database 11.2.0.4

- Applies protection at query execution time
- The stored data remain unchanged

  Redaction takes place immediately preceding the return of selected data and only at the top level of a SELECT list
- It is not an operation shown in the execution plan

Policy

```
SELECT rep.object_name  as "OBJECT",
       rep.policy_name,
       rep.expression,
       rep.enable,
       rec.column_name as "COLUMN",
       rec.function_type
 FROM redaction_policies rep,
      redaction_columns  rec
WHERE rep.object_owner = rec.object_owner
  AND rep.object_name  = rec.object_name;

OBJECT POLICY_NAME EXPRESSION                                        ENABLE COLUMN FUNCTION_TYPE
------ ----------- ------------------------------------------------ ------ ------ --------------
EMP    SCOTT_EMP   SYS_CONTEXT('SYS_SESSION_ROLES','MGR') = 'FALSE' YES    SALARY FULL REDACTION
```

```
SQL> EXPLAIN PLAN FOR SELECT * FROM EMP;
SQL> SELECT * FROM table(DBMS_XPLAN.DISPLAY(format=>'ALL'));
```

As SCOTT with the MGR role:

```
-------------------------------------------------------------------------------
| Id  | Operation          | Name | Rows  | Bytes | Cost (%CPU)|     Time |
-------------------------------------------------------------------------------
|   0 | SELECT STATEMENT   |      |     3 |    36 |     3   (0)| 00:00:01 |
|   1 |  TABLE ACCESS FULL| EMP  |     3 |    36 |     3   (0)| 00:00:01 |
-------------------------------------------------------------------------------
```

As SCOTT without the MGR role:

```
-------------------------------------------------------------------------------
| Id  | Operation          | Name | Rows  | Bytes | Cost (%CPU)|    Time  |
-------------------------------------------------------------------------------
|   0 | SELECT STATEMENT   |      |     3 |    36 |     3   (0)| 00:00:01 |
|   1 |  TABLE ACCESS FULL| EMP  |     3 |    36 |     3   (0)| 00:00:01 |
-------------------------------------------------------------------------------
```

Not to be confused with Oracle Data Masking

With Oracle Data Masking, the data is processed using masked shapes and this updated data is stored in new data blocks. For this reason, Data Masking is more suitable for **non-production** environments.

** Oracle Data Masking is available only with Enterprise Edition database and it requires licensing of Advanced Security.

Oracle Data Masking – Secure Your Nonproduction Environments

- Introduced in 10G;
- Designed to hide sensitive data during the copy from production to non-production;
- Useful to create environments like Development, Testing, UAT, etc;

Oracle Data Masking – Secure Your Nonproduction Environments

- Replaces the real data based on masking rules, like: Credit Card numbers, names, phone, address, social security number, etc;

- Compliance with regulatory requirements: (Sarbanes - Oxley, PCI DSS or HIPAA);

Oracle Data Masking

Production

LAST_NAME	SSN	SALARY
AGUILAR	203-33-3234	40,000
BENSON	323-22-2943	60,000

Non-Production

LAST_NAME	SSN	SALARY
ANSKEKSL	111—23-1111	60,000
BKJHHEIEDK	222-34-1345	40,000

Sensitive Data Never Leaves Database

Source: Oracle Documentation

Below are some other features that already existed to help making the data more secure:

- **Virtual Private Database (VPD)** - Allows control access on both row and column levels by dynamically adding a predicate to SQL statements issued against the database.
- **Oracle Label Security** – Allows you to add user-defined values to table records combining it with VPD to allow fine control of who sees what.
- **Database Vault** – Data Redaction does not prevent privileged users (such as DBAs) from having access to the data being protected. To solve this, you can make use of Database Vault.

Planning on Oracle Data Redaction Policy

1. Ensure that you have been granted the **EXECUTE** privilege on the **DBMS_REDACT** PL/SQL package.
2. Determine the **data type** of the table or view column that you want to redact.
3. Ensure that this column **is not used** in an Oracle Virtual Private Database (VPD) row filtering condition. That is, it must not be part of the VPD predicate generated by the VPD policy function.
4. Decide on the **type of redaction** that you want to perform: full, random, partial, regular expressions, or none.
5. Decide **which users** to apply the Data Redaction policy to.
6. Based on this information, create the Data Redaction policy by using the **DBMS_REDACT.ADD_POLICY** procedure.
7. Configure the policy to have additional columns to be redacted

Conditional Redaction Examples

- User Environment

```
expression => 'SYS_CONTEXT(''USERENV'',''SESSION_USER'') = ''SMITH'''
```

- Database Role

```
expression => 'SYS_CONTEXT(''SYS_SESSION_ROLES'',''SUPERVISOR'') = ''FALSE'''
```

- Oracle Label Security Label Dominance

```
expression => 'OLS_LABEL_DOMINATES (''hr_ols_pol'',''hs'') = 0'
```

- Application Express Session States

```
expression => 'V(''APP_USER'') != ''mavis@example.com'' or V(''APP_USER'') is null'
```

DBMS_REDACT

- DBMS_REDACT.ALTER_POLICY
  Allows changes to existing policies.

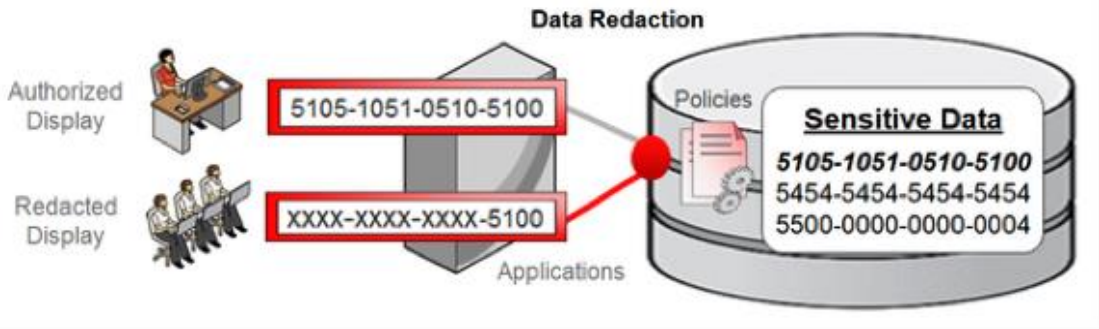
- DBMS_REDACT.DISABLE_POLICY
  Disables an existing policy.

- DBMS_REDACT.DROP_POLICY
  Drop an existing policy.

- DBMS_REDACT.ENABLE_POLICY
  Enables an existing policy.

- DBMS_REDACT.UPDATE_FULL_REDACTION_VALUES
  Change the default return value for full redaction.
  You **must restart the database** to take effect.

Accenture Enkitec Group



Redaction Methods

- Full redaction
- Partial redaction
- **Regular expressions**
- Random redaction
- No redaction

FULL Data Redaction

- Character Data Types

The output text is a single space

Column	Real Value	Redacted Value
Last_Name	Smith	‘ ‘

FULL Data Redaction

- Number Data Types

The output text is a zero

Column	Real Value	Redacted Value
Salary	8000	0

FULL Data Redaction

- Date-Time Data Types

The output text is set to the first day of January, 2001

Column	Real Value	Redacted Value
BirthDay	01/Dec/1980	01/Jan/2001

RANDOM Data Redaction

- CHAR Data Types

  Redacted in same character set and byte length as the column definition

Select 1

Column	**Real Value**	**Redacted Value**
Last_Name	Smith	Txaqw

Select 2

Column	**Real Value**	**Redacted Value**
Last_Name	Smith	Wascq

RANDOM Data Redaction

- Number Data Types

Redacted in same character set and the length is limited based on the length of the actual data

Select 1

Column	Real Value	Redacted Value
Salary	8000	4321

Select 2

Column	Real Value	Redacted Value
Salary	8000	6789

RANDOM Data Redaction

- Date-Time Data Types

  Redacted as random dates that are always different from those of the actual data

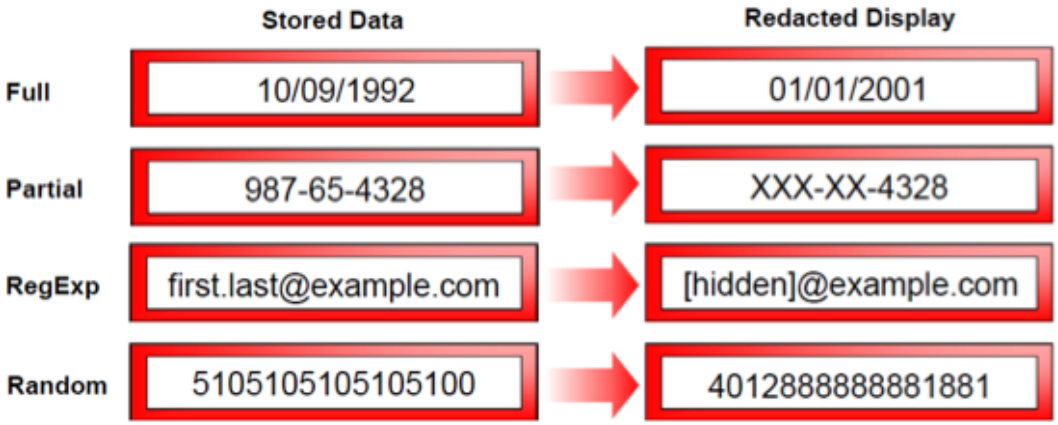
Select 1

Column	**Real Value**	**Redacted Value**
BirthDay	01/Dec/1980	10/Oct/1960

Select 2

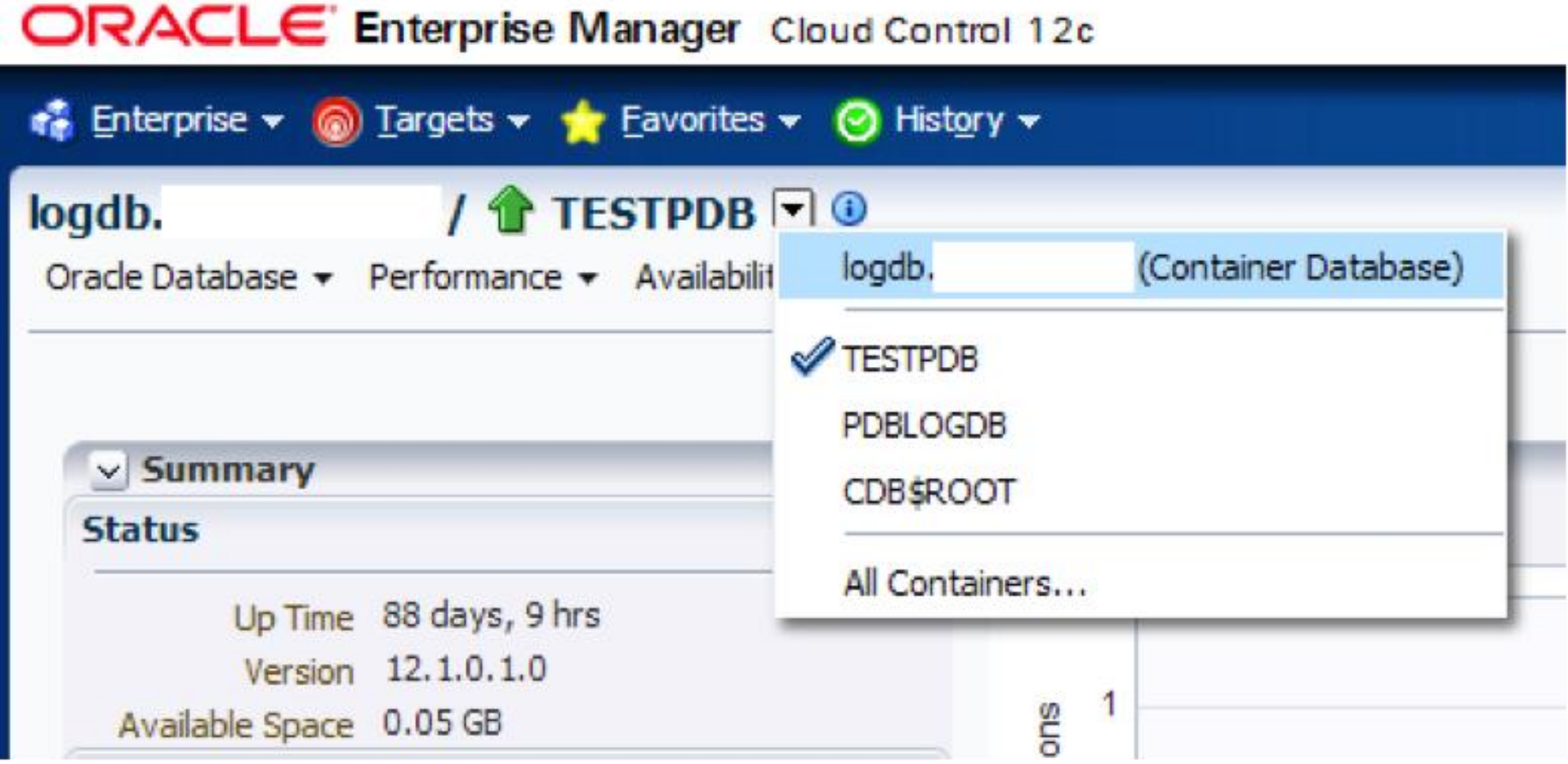
Column	**Real Value**	**Redacted Value**
BirthDay	01/Dec/1980	30/Aug/1932

Accenture Enkitec Group



Column data types

NUMBER, BINARY_FLOAT, BINARY_DOUBLE, CHAR, VARCHAR2, NCHAR, NVARCHAR2, DATE, TIMESTAMP, TIMESTAMP WITH TIME ZONE, BLOB, CLOB, and NCLOB

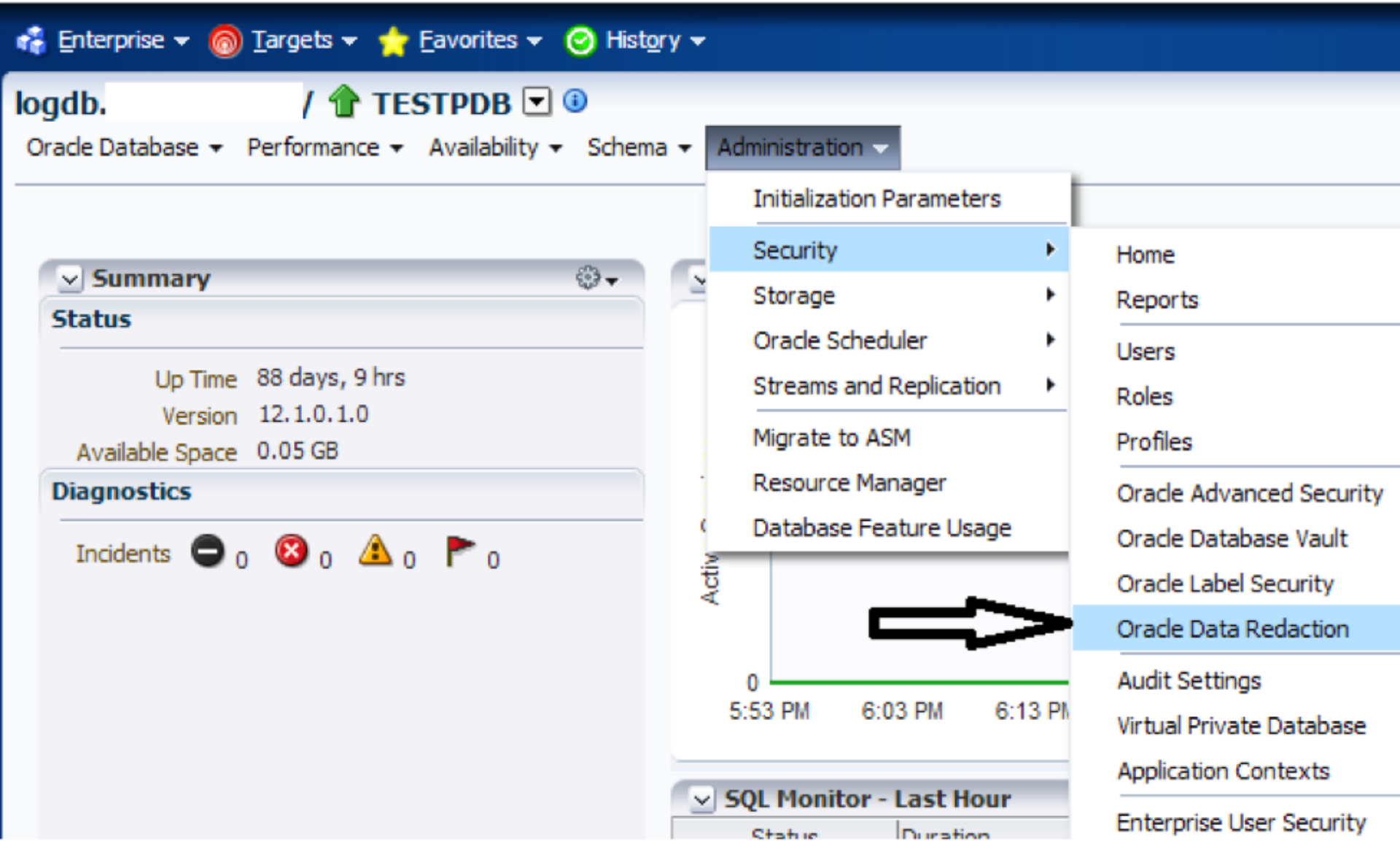

ORACLE Enterprise Manager Cloud Control 12c
Enterprise
Targets
Favorites
History
logdb.
/ TESTPDB
Oracle Database
Performance
Availabilit
logdb. (Container Database)
TESTPDB
PDBLOGDB
CDB$ROOT
All Containers...
Summary
Status
Up Time 88 days, 9 hrs
Version 12.1.0.1.0
Available Space 0.05 GB
ons
1

accenture
High performance. Delivered.

Accenture Enkitec Group

ORACLE TECHNOLOGY NETWORK LatinAmerica

ORACLE Enterprise Manager Cloud Control 12c



accenture
High performance. Delivered.

ORACLE TECHNOLOGY NETWORK LatinAmerica

Accenture Enkitec Group

ORACLE Enterprise Manager Cloud Control 12c

Enterprise Targets Favorites History

logdb / TESTPDB

Oracle Database Performance Availability Schema Administration

Data Redaction

Oracle Data Redaction provides an easy way to quickly redact sensitive information that is displayed in applications without altering the u
time according to flexible multi-factor policies.

Search Data Redaction Policies

Schema %

Table/View %

Policy Name %

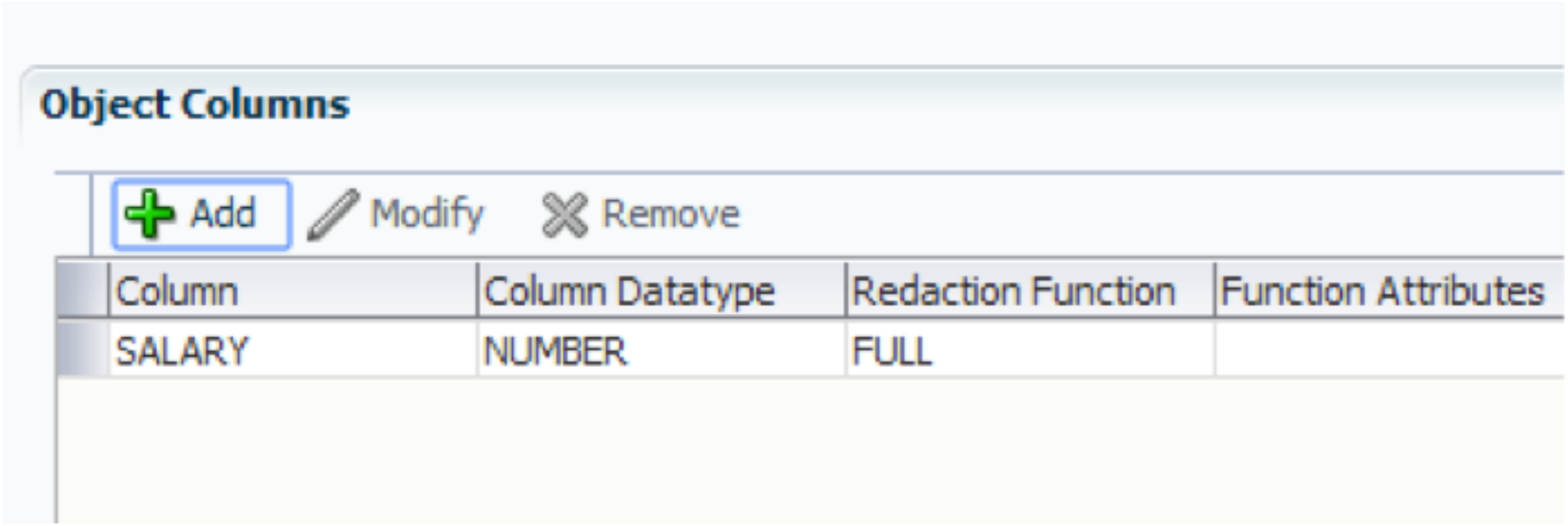
Go

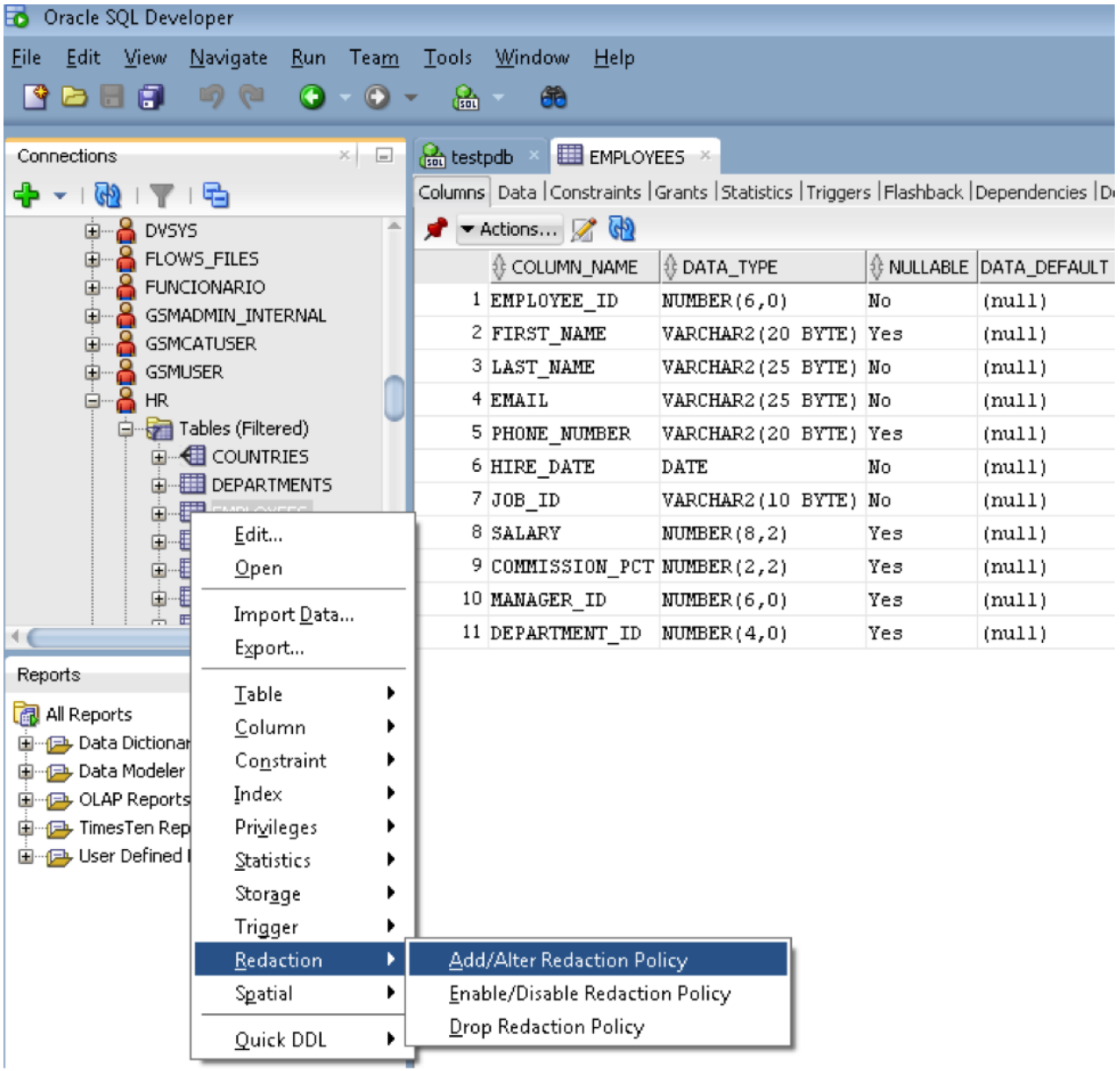
Data Redaction Policies

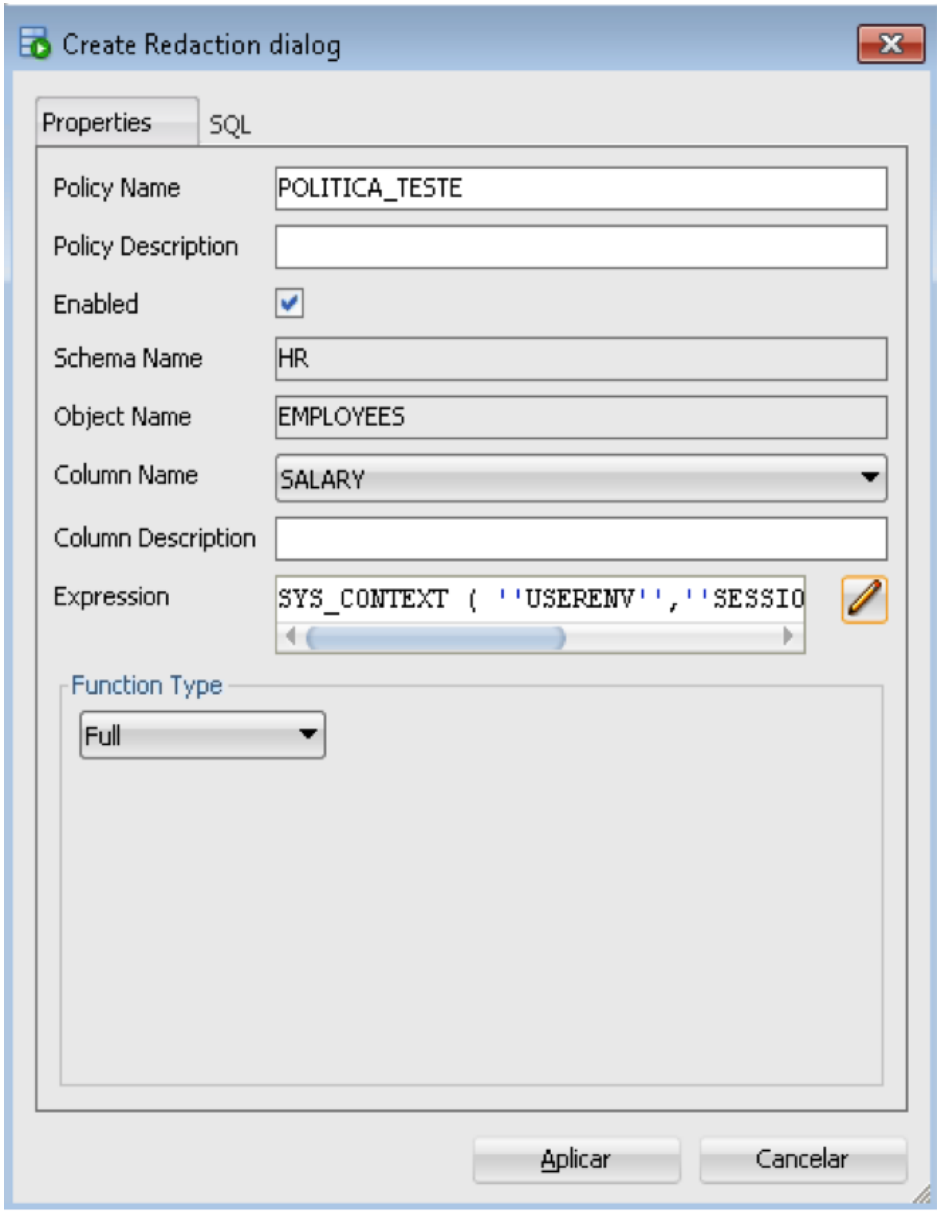
Create Edit View Enable Disable Delete

Schema	Table/View	Policy Name	Enabled	Redacted Columns


ORACLE Enterprise Manager Cloud Control 12c
Enterprise
Targets
Favorites
History
logdb.
/ TESTPDB
Oracle Database
Performance
Availability
Schema
Administration
Create Data Redaction Policy: POLITICA_TESTE
* Schema
HR
* Table/View
EMPLOYEES
* Policy Name
POLITICA_TESTE
* Policy Expression
SYS_CONTEXT('USERENV', 'SESSION_USER') != 'SUPERVISOR'


Object Columns
Add
Modify
Remove
Column
Column Datatype
Redaction Function
Function Attributes
SALARY
NUMBER
FULL


Oracle SQL Developer
File Edit View Navigate Run Team Tools Window Help
Connections
DVSYS
FLOWS_FILES
FUNCIONARIO
GSMADMIN_INTERNAL
GSMCATUSER
GSMUSER
HR
Tables (Filtered)
COUNTRIES
DEPARTMENTS
Reports
All Reports
Data Dictionar
Data Modeler
OLAP Reports
TimesTen Rep
User Defined
testpdb
EMPLOYEES
Columns Data Constraints Grants Statistics Triggers Flashback Dependencies
Actions...
COLUMN_NAME DATA_TYPE NULLABLE DATA_DEFAULT
1 EMPLOYEE_ID NUMBER(6,0) No (null)
2 FIRST_NAME VARCHAR2(20 BYTE) Yes (null)
3 LAST_NAME VARCHAR2(25 BYTE) No (null)
4 EMAIL VARCHAR2(25 BYTE) No (null)
5 PHONE_NUMBER VARCHAR2(20 BYTE) Yes (null)
6 HIRE_DATE DATE No (null)
7 JOB_ID VARCHAR2(10 BYTE) No (null)
8 SALARY NUMBER(8,2) Yes (null)
9 COMMISSION_PCT NUMBER(2,2) Yes (null)
10 MANAGER_ID NUMBER(6,0) Yes (null)
11 DEPARTMENT_ID NUMBER(4,0) Yes (null)
Edit...
Open
Import Data...
Export...
Table
Column
Constraint
Index
Privileges
Statistics
Storage
Trigger
Redaction
Spatial
Quick DDL
Add/Alter Redaction Policy
Enable/Disable Redaction Policy
Drop Redaction Policy


Create Redaction dialog
Properties
SQL
Policy Name
POLITICA_TESTE
Policy Description
Enabled
Schema Name
HR
Object Name
EMPLOYEES
Column Name
SALARY
Column Description
Expression
SYS_CONTEXT (''USERENV'',''SESSIO
Function Type
Full
Aplicar
Cancelar

```
SQL>

BEGIN

 DBMS_REDACT.ADD_POLICY  (OBJECT_SCHEMA => 'HR',  object_name => 'EMPLOYEES',  policy_name =>
'POLITICA_TESTE',  expression => 'SYS_CONTEXT(''USERENV'', ''SESSION_USER'') != ''SUPERVISOR''');

 DBMS_REDACT.ALTER_POLICY  (OBJECT_SCHEMA => 'HR',  object_name => 'EMPLOYEES',  policy_name =>
'POLITICA_TESTE',  action => DBMS_REDACT.ADD_COLUMN,  column_name => '"SALARY"',
 function_type => DBMS_REDACT.FULL );


END;
 /

PL/SQL procedure successfully completed.
```

Operational Activities - No Redaction

- Backup and Restore
- Import and Export
- Patching and Upgrades
- Replication
- **Users SYS and SYSTEM automatically have the `EXEMPT REDACTION POLICY` system privilege**
- **Data Redaction is not enforced for users connected as `SYSDBA`**

Data Redaction and Data Pump

```
ORA-28081: Insufficient privileges - the command
   references a redacted object
```

Use the `EXEMPT REDACTION POLICY` system privilege in these cases. However, use it with caution.

Note that the role `DATAPUMP_EXP_FULL_DATABASE` includes the `EXEMPT REDACTION POLICY` system privilege

Data Redaction and CTAS

If you try to CREATE TABLE ... AS SELECT (CTAS) against a redacted table you get the following error message: **ORA-28081: Insufficient privileges - the command references a redacted object.**

In order to perform a `CREATE TABLE AS SELECT` operation from a table protected by an active redaction policy, the user must have privileges to see the actual data on the source table

Because applications may need to perform `CREATE TABLE AS SELECT` operations that involve redacted source columns, you can grant the application the `EXEMPT DDL REDACTION POLICY` system privilege.

Redacted Columns and GROUP BY SQL Expressions

Redacted Columns included in SQL expressions on a GROUP BY clause will fail as follows:

```
SQL> select * from emp;

    EMP_NO NAME                                      SALARY
---------- ---------------------------------------- ----------
         1 Daniel                                   702
         2 Juca                                     607
         3 Manuel                                   314

SQL> select (salary*1.10) from emp group by (salary*1.10);
select (salary*1.10) from emp group by (salary*1.10)
        *
ERROR at line 1:
ORA-00979: not a GROUP BY expression
```

Redacted Columns and Virtual Columns

```
SQL> alter table hr.employees add sal number as (salary*1.10) virtual;

alter table hr.employees add sal number as (salary*1.10) virtual
*
ERROR at line 1:
ORA-28083: A redacted column was referenced in a virtual column expression.
```

Data Redaction and Views

- Columns from MVIEWS as well as regular VIEWS can be redacted

Overhead

- It could reach up to 10% of performance impact when using complex Regular Expressions
- Between 2-3% performance impact using other redaction methods

Hacking

- Never to be considered as a way to protect data from **anyone with SQL access** to the database

- Extremely easy to hack **once you have access to SQL**

accenture
High performance. Delivered.

ORACLE TECHNOLOGY NETWORK LatinAmerica

Accenture Enkitec Group

accenture
High performance. Delivered.

ORACLE TECHNOLOGY NETWORK LatinAmerica

Accenture Enkitec Group

Time for SQLcl ?

Oracle SQL Developer 4.1 EA2 (4.1.0.18.37)

March 9, 2015

Thank you for accepting the OTN License Agreement; you may now download this software.

- Bugs Fixed
- Release Notes
- New Features
- Documentation

SQL Developer requires JDK 8	Java 8 Download Page
Platform	
Windows 32/64-bit - Installation Notes	**Download** 307 M
Mac OS X - Installation Notes	**Download** 307 M
Linux RPM - Installation Notes	**Download** 301 M
Other Platforms - Installation Notes	**Download** 307 M

Command Line - SQLcl ***Update Apr 16, 2015***	
All Platforms	**Download** 12 M
• Over 350+ Bugs Fixed	
Getting Started Video	

accenture
High performance. Delivered.

ORACLE
TECHNOLOGY NETWORK
LatinAmerica

Accenture Enkitec Group

Thank You