Oracle Data Redaction

# Redacting Protected Column Values with FULL Redaction

1. Display the current values from the HR.EMPLOYEES table before redaction.

$ sqlplus system

Enter password: \*\*\*\*\*\*

Connected to:

Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 -

64bit Production

With the Partitioning, OLAP, Advanced Analytics, Real

Application Testing and Unified Auditing options

SQL> SELECT employee\_id, last\_name, salary

FROM hr.employees

WHERE department\_id = 100;

EMPLOYEE\_ID LAST\_NAME SALARY

----------- --------------------- ----------

108 Greenberg 12008

109 Faviet 9000

110 Chen 8200

111 Sciarra 7700

112 Urman 7800

113 Popp 6900

6 rows selected.

SQL>

1. Define a masking policy for the HR.EMPLOYEES table specifying full masking for the SALARY column. SALARY is defined as NUMBER(8,2). In this example, by setting EXPRESSION to 1=1, redaction is always performed because the expression always evaluates to true.

The policy is enabled by default.

BEGIN

DBMS\_REDACT.ADD\_POLICY

(object\_schema => 'HR',

object\_name => 'EMPLOYEES',

policy\_name => 'EMPSAL\_POLICY',

column\_name => 'SALARY',

function\_type => DBMS\_REDACT.FULL,

expression => '1=1');

END;

/

1. Query REDACTION\_POLICIES to verify that the policy has been created and is enabled. This view also shows under what condition the redaction will be performed as shown in the EXPRESSION column. Use the following column formats.

COL object\_owner FORMAT A12

COL object\_name FORMAT A12

COL policy\_name FORMAT A14

COL expression FORMAT A12

COL enable FORMAT A6

COL policy\_description FORMAT A10

COL column\_name FORMAT A10

COL function\_type FORMAT A17

COL function\_parameters FORMAT A20

SQL> **SELECT \* FROM redaction\_policies;**  
OBJECT\_OWNER OBJECT\_NAME POLICY\_NAME EXPRESSION ENABLE  
------------ ------------ -------------- ------------ ------  
POLICY\_DES  
----------  
HR EMPLOYEES EMPSAL\_POLICY 1=1 YES

1. Display which columns will be redacted and what type of redaction will take place.

SQL> SELECT object\_owner, object\_name, column\_name,  
function\_type, function\_parameters  
FROM redaction\_columns;  
  
OBJECT\_OWNER OBJECT\_NAME COLUMN\_NAM FUNCTION\_TYPE  
------------ ---------------- ---------- -----------------  
FUNCTION\_PARAMETERS  
--------------------  
HR EMPLOYEES SALARY FULL REDACTION

1. Now query the HR.EMPLOYEES table again and note that the value of the SALARY column is 0 for all displayed rows.

* First grant the SELECT privilege to SH.

SQL> GRANT select ON hr.employees TO sh;

Grant succeeded.

* Connect as SH. If SH is locked, unlock the account.

SQL> ALTER USER sh IDENTIFIED BY sh ACCOUNT UNLOCK;

User altered.

SQL> CONNECT sh/sh

Connected.

* Run the same select as in task 1

SQL> SELECT employee\_id, last\_name, salary   
FROM hr.employees  
WHERE department\_id = 100;  
EMPLOYEE\_ID LAST\_NAME SALARY  
----------- ------------------------- ----------  
108 Greenberg 0  
109 Faviet 0  
110 Chen 0  
111 Sciarra 0  
112 Urman 0  
113 Popp 0  
6 rows selected.

1. If you query as SYSDBA, the “real” value is displayed, not the redacted value as shown in this example. Any user who is granted the EXEMPT REDACTION POLICY privilege bypasses any redaction policy.

* Connect as SYSDBA.

SQL> CONNECT / AS SYSDBA

Connected.

SQL>

* Run the same select as in task 1.

SQL> /

EMPLOYEE\_ID LAST\_NAME SALARY

----------- ------------------------- ----------

108 Greenberg 12008

109 Faviet 9000

110 Chen 8200

111 Sciarra 7700

112 Urman 7800

113 Popp 6900

6 rows selected.

SQL

# Redacting Protected Column Values with PARTIAL Redaction

1. Query the HR.EMPLOYEES table again and display the HIRE\_DATE column.

SQL> SELECT employee\_id, last\_name, hire\_date

FROM hr.employees

WHERE department\_id = 100;

EMPLOYEE\_ID LAST\_NAME HIRE\_DATE

----------- ------------------------- ---------

108 Greenberg 17-AUG-02

109 Faviet 16-AUG-02

110 Chen 28-SEP-05

111 Sciarra 30-SEP-05

112 Urman 07-MAR-06

113 Popp 07-DEC-07

2. Alter the masking policy to redact the HIRE\_DATE column. In this example, partial redaction is used to mask the actual year of hire.

BEGIN

DBMS\_REDACT.ALTER\_POLICY

(object\_schema => 'HR',

object\_name => 'EMPLOYEES',

policy\_name => 'EMPSAL\_POLICY',

action => DBMS\_REDACT.ADD\_COLUMN,

column\_name => 'HIRE\_DATE',

function\_type => DBMS\_REDACT.PARTIAL,

function\_parameters=> 'MDy2012',

expression => '1=1');

END;

/

3. Query REDACTION\_POLICIES to verify that the policy has been created and is enabled. This view also shows under what condition the redaction will be performed as shown in the EXPRESSION column.

SQL> select \* from redaction\_policies;

OBJECT\_OWNER OBJECT\_NAME POLICY\_NAME EXPRESSION ENABLE

------------ ------------ ----------------- ---------- ------

POLICY\_DES

----------

HR EMPLOYEES EMPSAL\_POLICY 1=1 YES

SQL>

4. The REDACTION\_COLUMNS view shows both masking functions defined on the HR.EMPLOYEES table.

SQL> SELECT object\_owner, object\_name, column\_name,

function\_type, function\_parameters

FROM redaction\_columns;

OBJECT\_OWNER OBJECT\_NAME COLUMN\_NAM FUNCTION\_TYPE

------------ ------------ ---------- ----------------

FUNCTION\_PARAMETERS

--------------------

HR EMPLOYEES SALARY FULL REDACTION

HR EMPLOYEES HIRE\_DATE PARTIAL REDACTION

MDy2012

SQL>

5. Query HR.EMPLOYEES again as the SH user. ’12’ is displayed as the hire year for all the rows selected.

SQL> CONNECT sh

Enter password: \*\*\*\*\*\*

Connected.

SQL> select employee\_id, last\_name, hire\_date

from hr.employees

where department\_id = 100;

EMPLOYEE\_ID LAST\_NAME HIRE\_DATE

----------- ------------------------- ---------

108 Greenberg 17-AUG-12

109 Faviet 16-AUG-12

110 Chen 28-SEP-12

111 Sciarra 30-SEP-12

112 Urman 07-MAR-12

113 Popp 07-DEC-12

6 rows selected.

# Cleaning Up Redaction Policies

1. Drop the redaction policy as SYSTEM user.

BEGIN

DBMS\_REDACT.DROP\_POLICY

(object\_schema => 'HR',

object\_name => 'EMPLOYEES',

policy\_name => 'EMPSAL\_POLICY');

END;

/

SQL> CONNECT system

Enter password: \*\*\*\*\*\*

Connected.

SQL> BEGIN

DBMS\_REDACT.DROP\_POLICY

(object\_schema => 'HR',

object\_name => 'EMPLOYEES',

policy\_name => 'EMPSAL\_POLICY');

END;

/

2. Check that the values for the SALARY and HIRE\_DATE columns are displayed without redaction.

SQL> select employee\_id, last\_name, salary, hire\_date

from hr.employees

where department\_id = 100;

2 3

EMPLOYEE\_ID LAST\_NAME SALARY HIRE\_DATE

----------- ------------------------- ---------- ---------

108 Greenberg 12008 17-AUG-02

109 Faviet 9000 16-AUG-02

110 Chen 8200 28-SEP-05

111 Sciarra 7700 30-SEP-05

112 Urman 7800 07-MAR-06

113 Popp 6900 07-DEC-07

6 rows selected.

SQL> EXIT

# Changing the Default Value for FULL Redaction

1. Modify the default value to 10 for full redaction of the commission percentage of all employees.

* Display the information from the data dictionary view before updating the default value.

$ sqlplus / AS SYSDBA

SQL> SELECT number\_value FROM REDACTION\_VALUES\_FOR\_TYPE\_FULL;

NUMBER\_VALUE

------------

0

* Modify the default value.

SQL> exec DBMS\_REDACT.UPDATE\_FULL\_REDACTION\_VALUES( -

NUMBER\_VAL => 10)

PL/SQL procedure successfully completed.

SQL>

* Display the information from the data dictionary view.

SQL> SELECT number\_value FROM REDACTION\_VALUES\_FOR\_TYPE\_FULL;

NUMBER\_VALUE

------------

10

SQL>

* Add the COMMISSION\_PCT column to the policy for full redaction using the following code.

BEGIN

DBMS\_REDACT.ADD\_POLICY

(object\_schema => 'HR',

object\_name => 'EMPLOYEES',

policy\_name => 'EMPCOMM\_POLICY',

column\_name => 'COMMISSION\_PCT',

function\_type => DBMS\_REDACT.FULL,

expression => '1=1');

END;

/

2. After you modify a value, you must restart the database for it to take effect. If you only flush the buffer cache, the real value of the column will be displayed.

SQL> CONNECT / AS SYSDBA

Connected.

SQL> SHUTDOWN IMMEDIATE

Database closed.

Database dismounted.

ORACLE instance shut down.

SQL> STARTUP

ORACLE instance started.

Total System Global Area 503316480 bytes

Fixed Size 2916056 bytes

Variable Size 272630056 bytes

Database Buffers 222298112 bytes

Redo Buffers 5472256 bytes

Database mounted.

Database opened.

SQL>

3. Display the values of the COMMISSION\_PCT column of all employees.

SQL> SELECT commission\_pct, first\_name FROM hr.employees

ORDER BY 1 DESC;

2

COMMISSION\_PCT FIRST\_NAME

-------------- --------------------

… rows deleted …

Shelley

William

10 John

10 Allan

10 Patrick

10 Ellen