Herr der Daten:
APEX, VPD und Data Redaction – Die Gefährten.

Dr. Thomas Petrik, November 2024

Über Sphinx

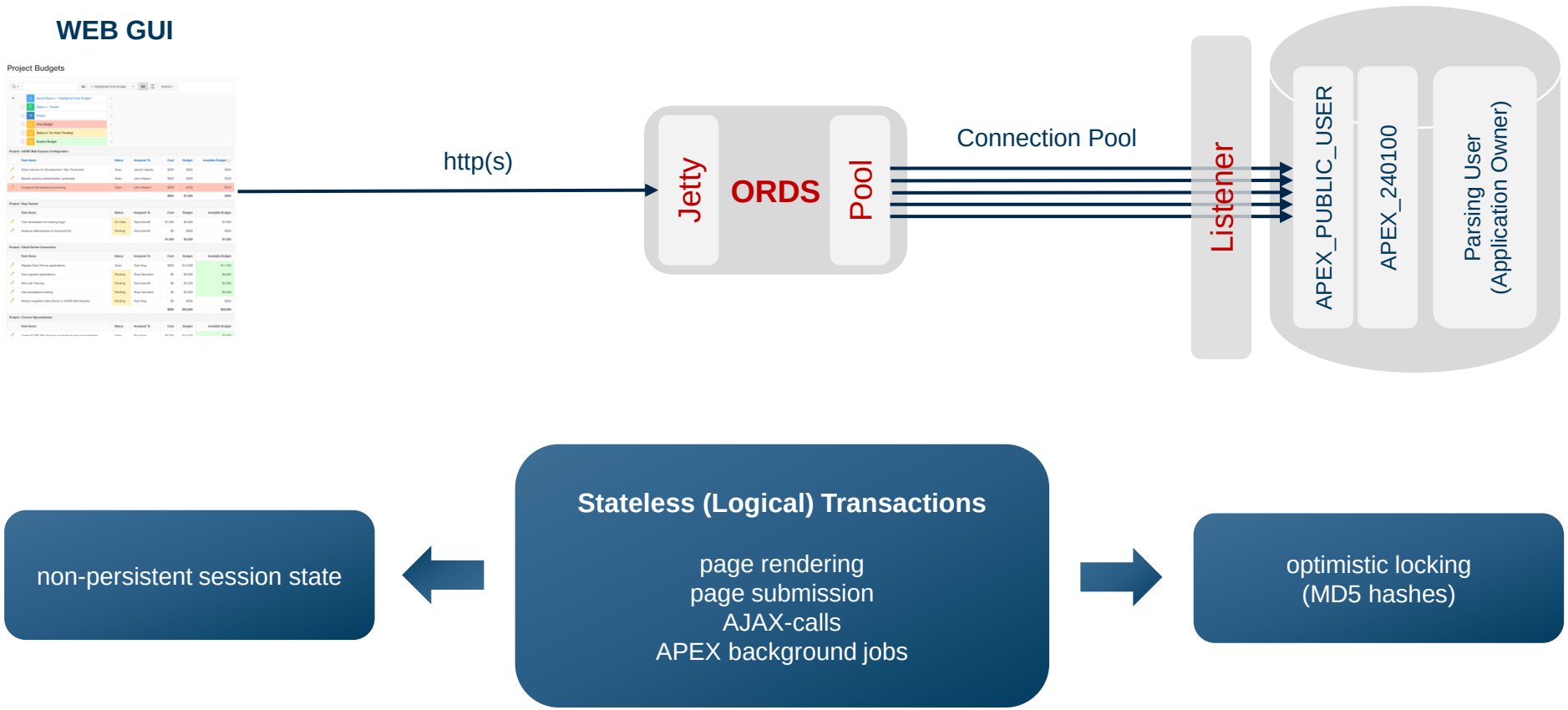
Joy, Performance & Passion for Perfection

- **Gegründet:**
  1994 Sphinx IT-Consulting GmbH
  2003 Sphinx Managed Services GmbH
  eigentümergeführt
- **Firmensitz:** Wien
- **Was wir tun:** Realisierung wegweisender & nachhaltig wirksamer IT-Lösungen in erstaunlich kurzer Zeit.
- **Unsere Philosophie:** Ganzheitliche Beratung, maßgeschneiderte Lösungen, Wertschätzung bestehender Systeme und für die Menschen dahinter.
- **Geschäftsbereiche:**
  - Analytics & Business Intelligence
  - Infrastruktur & Datenbanktechnologie
  - IT- & Data Security
  - IT- & Prozessautomatisierung
  - AI in Business-Lösungen
  - Strategische Beratung & externe IT

"The Path to the Precious"

APEX Architecture & Session Handling

APEX Architecture



APEX Session Handling & Authorization

```
SELECT sid
      ,serial#
      ,username
      ,client_info
      ,client_identifier
      ,program
  FROM v$session
 WHERE username = 'APEX_PUBLIC_USER'
```

SID	SERIAL#	USERNAME	CLIENT_INFO	CLIENT_IDENTIFIER	PROGRAM
209	43824	APEX_PUBLIC_USER	1815905510179347:e002881	e002881:124400992628492	Oracle REST Data Services

APEX_240100.WWV_FLOW_*
(via PUBLIC synonym)

SYS.WWV_DBMS_SQL_APEX_240100

SYS.DBMS_SYS_SQL

execute as "Parsing User"

impersonation to workspace SCHEMA

```
PROCEDURE PARSE_AS_USER(C             IN INTEGER,
                        STATEMENT     IN VARCHAR2,
                        LANGUAGE_FLAG IN INTEGER,
                        USERID        IN INTEGER DEFAULT NULL);
```

Excursus: DBMS_SYS_SQL for the DBA

sudo for DBAs

```
PROCEDURE exec_sql_as_user (p_sql IN CLOB, p_username IN VARCHAR2)
   IS
       --
       -- execute a statement as any user
       --
       v_cur   INTEGER;
       v_uid   INTEGER;
   BEGIN
       IF p_username IS NULL
       THEN
           EXECUTE IMMEDIATE p_sql;
       ELSE
           SELECT user_id
             INTO v_uid
             FROM dba_users
            WHERE username = p_username;

           v_cur := DBMS_SQL.open_cursor;
           sys.DBMS_SYS_SQL.parse_as_user (v_cur
                                           ,p_sql
                                           ,DBMS_SQL.native
                                           ,v_uid);
           DBMS_SQL.close_cursor (v_cur);
       END IF;
END;
```

APEX Session Handling & Authorization

```
SELECT sid
      ,serial#
      ,username
      ,client_info
      ,client_identifier
      ,program
  FROM v$session
 WHERE username = 'APEX_PUBLIC_USER'
```

SID	SERIAL#	USERNAME	CLIENT_INFO	CLIENT_IDENTIFIER	PROGRAM
209	43824	APEX_PUBLIC_USER	1815905510179347:e002881	e002881:124400992628492	Oracle REST Data Services

Workspace-ID:APP_USER

APP_USER:Session-ID

https://nzapxt01:8180/ords/dwht/r/dwhexp/dwhexplorer/dashboard?session=124400992628492

- get values also using SYS_CONTEXT
  - sys_context('userenv', 'CLIENT_INFO')
  - sys_context('userenv', 'CLIENT_IDENTIFIER')
  - sys_context('APEX$SESSION', 'APP_USER')

APEX Session Handling & Authorization

```
SELECT workspace_id
      ,apex_session_id
      ,user_name
      ,session_created
      ,session_life_timeout_on
  FROM apex_workspace_sessions
```

based on
WWV_FLOW_SESSIONS$

contains
COOKIE_VALUE
CRYPTO_SALT
etc.

WORKSPACE_ID	APEX_SESSION_ID	USER_NAME	SESSION_CREATED	SESSION_LIFE_TIMEOUT_ON
1815905510179347	124400992628492	e002881	2024-11-16 14:10:25	2025-11-16 14:10:25

APP_USER

session reset:
cleanup local contexts and package variables

DBMS_SESSION.modify_package_state (DBMS_SESSION.reinitialize)

"The Fellowship"

In-Database-Security: VPD & Redaction

APEX In-Database-Security

Row Level Security

INSTITUTE	DEPARTMENT	…	AMOUNT
103	DEP2	…	300
196	DEP2	…	400
104	DEP2	…	10000

INSTITUTE	DEPARTMENT	…	AMOUNT
196	DEP2	…	400

select * from table;

department=DEP2

institute=196 and department=DEP2

INSTITUTE	DEPARTMENT	…	AMOUNT
196	DEP1	…	5000
103	DEP2	…	300
196	DEP2	…	400
104	DEP2	…	10000

Column Level Security

INSTITUTE	DEPARTMENT	…	AMOUNT
196	DEP1	…	(null)
103	DEP2	…	300
196	DEP2	…	(null)
104	DEP2	…	10000

INSTITUTE	DEPARTMENT	…	AMOUNT
196	DEP1	…	(null)
103	DEP2	…	(null)
196	DEP2	…	(null)
104	DEP2	…	(null)

select * from table;

sensitive columns only for INSTITUTE 103,104

no sensitive columns at all

INSTITUTE	DEPARTMENT	…	AMOUNT
196	DEP1	…	5000
103	DEP2	…	300
196	DEP2	…	400
104	DEP2	…	10000

RLS quickly explained

```
SYS.DBMS_RLS.ADD_POLICY      (
   object_schema           => Null
   ,object_name            => 'CLS_DEMO'
   ,policy_name            => 'SCURTY_VPD_SEC_TNT'
   ,function_schema        => 'SCURTY'
   ,policy_function        => 'F_VPD_SEC_TNT'
   ,statement_types        => 'SELECT'
   ,policy_type            => dbms_rls.dynamic
   ,long_predicate         => TRUE
   ,update_check           => FALSE
   ,enable                 => TRUE );
```

```
CREATE OR REPLACE FUNCTION SCURTY.f_vpd_sec_tnt (p_object_owner IN VARCHAR2
                                                ,p_object_name IN VARCHAR2)
    RETURN VARCHAR2
IS
    v_where   CLOB;
BEGIN
    BEGIN
        SELECT /*+ result_cache */
               tnt_code_expr
          INTO v_where
          FROM rep_vpd_tnt_access_rlt
         WHERE     username = SYS_CONTEXT ('APEX$SESSION', 'APP_USER')
               AND table_owner = p_object_owner
               AND table_name = p_object_name;

        RETURN v_where;
    EXCEPTION
        WHEN NO_DATA_FOUND
        THEN
            RETURN '1=2';
    END;
END f_vpd_sec_tnt;
```

config table

CLS quickly explained

```
SYS.DBMS_RLS.ADD_POLICY      (
   object_schema           => Null
   ,object_name            => 'CLS_DEMO'
   ,policy_name            => 'SCURTY_VPD_SCOL'
   ,function_schema        => 'SCURTY'
   ,policy_function        => 'F_VPD_SCOL'
   ,statement_types        => 'SELECT'
   ,policy_type            => dbms_rls.dynamic
   ,long_predicate         => FALSE
   ,sec_relevant_cols      => 'AMOUNT'
   ,sec_relevant_cols_opt => dbms_rls.all_rows
   ,update_check           => FALSE
   ,enable                 => TRUE );
```

```
CREATE OR REPLACE FUNCTION SCURTY.f_vpd_scol (p_object_owner    IN VARCHAR2
                                             ,p_object_name     IN VARCHAR2)
    RETURN VARCHAR2
IS
    v_where   VARCHAR2 (32767);
BEGIN
    BEGIN
        SELECT /*+ result_cache */
               tnt_code_expr
          INTO v_where
          FROM rep_vpd_scol_access_all
         WHERE     username = sys_context('APEX$SESSION','APP_USER')
               AND table_owner = p_object_owner
               AND table_name = p_object_name;

        RETURN v_where;
    EXCEPTION
        WHEN NO_DATA_FOUND
        THEN
            RETURN '1=2';
    END;
END f_vpd_scol;
```

config table

CLS – Statement Expansion

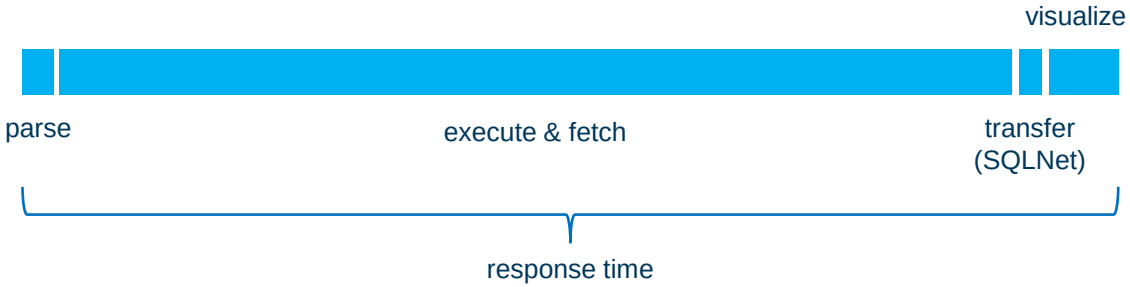
```
CREATE OR REPLACE FUNCTION expand_sql (p_sql IN CLOB)
    RETURN CLOB
IS
    v_out   CLOB;
BEGIN
    DBMS_UTILITY.expand_sql_text (input_sql_text => p_sql, output_sql_text => v_out);
    RETURN v_out;
END expand_sql;
/

SELECT expand_sql('select * from dwh.cls_demo')
  FROM dual;
```

```
SELECT "A1"."INSTITUTE"      "INSTITUTE"
      ,"A1"."DEPARTMENT"     "DEPARTMENT"
      ,"A1"."AMOUNT"         "AMOUNT"
  FROM (SELECT "A2"."INSTITUTE"      "INSTITUTE"
              ,"A2"."DEPARTMENT"     "DEPARTMENT"
              ,"A2"."AMOUNT"         "AMOUNT"
          FROM (SELECT "A3"."INSTITUTE"     "INSTITUTE"
                      ,"A3"."DEPARTMENT"    "DEPARTMENT"
                      ,CASE
                           WHEN (   "A3"."INSTITUTE" = 103
                                 OR "A3"."INSTITUTE" = 104)
                           THEN
                               "A3"."AMOUNT"
                           ELSE
                               NULL
                       END                   "AMOUNT"
                  FROM (SELECT "A4"."INSTITUTE"      "INSTITUTE"
                              ,"A4"."DEPARTMENT"     "DEPARTMENT"
                              ,"A4"."AMOUNT"         "AMOUNT"
                          FROM "DWH"."CLS_DEMO" "A4"
                         WHERE    "A4"."INSTITUTE" = 103
                               OR "A4"."INSTITUTE" = 104
                               OR "A4"."INSTITUTE" = 196) "A3") "A2") "A1"
```

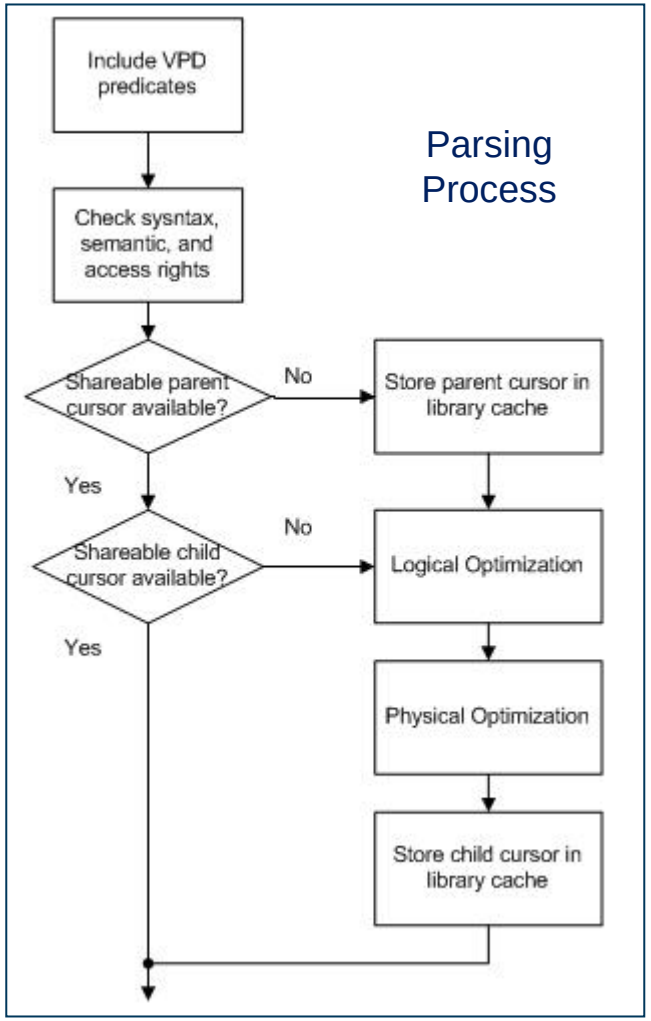
CLS

RLS

VPD Performance Impact



- VPD adds to the parse time only
  longer runtime - less impact
- avg. runtime of a policy function: 165 ns
- estimated impact:
  e.g. 5 tables accessed
  5 x 165 ns + some policy overhead ≈ 1 ms
  < 1% for all queries with a response time > 100 ms
  additional policies may add some overhead
  in many cases policy functions are exited in an early stage



Christian Antognini, Troubleshooting Oracle Performance

Data Redaction

```
BEGIN
  SYS.DBMS_REDACT.ADD_POLICY (
    object_schema       => 'DWH',
    object_name         => 'CLS_DEMO',
    policy_name         => 'SCURTY_DR',
    expression          => 'sys_context(''CTX_DR'',''91439'') = 1',
    policy_description => '',
    enable              => TRUE);

  SYS.DBMS_REDACT.ALTER_POLICY (
    object_schema           => 'DWH',
    action                  => SYS.DBMS_REDACT.ADD_COLUMN,
    object_name             => 'CLS_DEMO',
    policy_name             => 'SCURTY_DR',
    column_name             => 'AMOUNT',
    function_type           => SYS.DBMS_REDACT.RANDOM);
END;
```

- Data Redaction is based on simple expressions.
  - NO functions (like VPD)
  - NO configuration tables
- Data Redaction operates on the result set
  - does not change the execution plan
  - column is masked but still works in where-clauses
  - is not secure if users can access the DB via SQL
    - User may try out several where clauses in order to classify and guess the content of as column.
- Perfect solution for APEX
  - transparent masking
  - very flexible masking options
  - columns are not just empty

Make Data Redaction flexible via VPD

```
BEGIN
  SYS.DBMS_REDACT.ADD_POLICY (
    object_schema      => 'DWH',
    object_name        => 'CLS_DEMO',
    policy_name        => 'SCURTY_DR',
    expression         => 'sys_context(''CTX_DR'',''91439'') = 1',
    policy_description => '',
    enable             => TRUE);
…
```

object ID

SELECT

execute first VPD
set context for object

Redaction policy reacts on
changed context

first CLS-VPD

```
CREATE OR REPLACE FUNCTION SCURTY.f_vpd_mcol (p_object_owner IN VARCHAR2
                                             ,p_object_name IN VARCHAR2)
    RETURN VARCHAR2
IS
…
BEGIN
    BEGIN
        SELECT /*+ result_cache */
               object_id
          INTO v_object_id
          FROM rep_vpd_mcol_access
         WHERE     username = SYS_CONTEXT ('APEX$SESSION', 'APP_USER')
               AND table_owner = p_object_owner
               AND table_name = p_object_name;

        v_mcol_access := 1;
    EXCEPTION
        WHEN NO_DATA_FOUND
        THEN
            SELECT /*+ result_cache */
                   object_id
              INTO v_object_id
              FROM dba_objects
             WHERE object_owner = p_object_owner AND object_name = p_object_name;

            v_mcol_access := 0;
    END;

    DBMS_SESSION.set_context ('CTX_DR', v_object_id, v_mcol_access);

    IF v_mcol_access = 1
    THEN
        RETURN '1=1';
    ELSE
        RETURN f_vpd_scol (p_object_owner, p_object_name);
    END IF;
END f_vpd_mcol;
```

show all MASKED values

call second CLS-VPD if
masking is not required

Make Data Redaction flexible via VPD

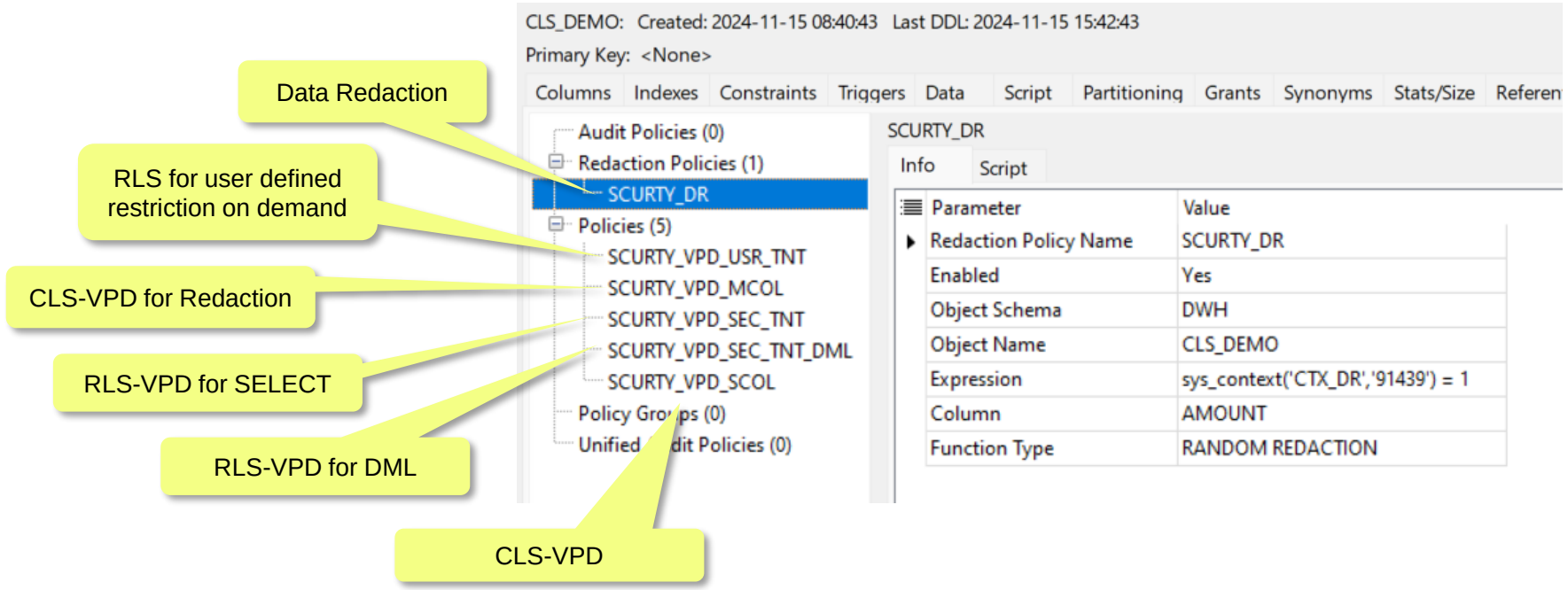
```
SELECT * FROM dwh.cls_demo
```

INSTITUTE	DEPARTMENT	AMOUNT	AMOUNT_2
196	DEP1	4823	
103	DEP2	12	300
196	DEP2	158	
104	DEP2	2788	10000

Data Redaction random masking

second CLS-VPD column NOT redacted

Everything combined



Depending on the Oracle version you may hit ORA-28094:

ORA-28094: SQL construct not supported by data redaction

Solution:
Set hidden parameter "_strict_redaction_semantics" to FALSE.

see also: https://mvelikikh.blogspot.com/2021/03/strict-redaction-semantics.html

APEX: Preserving Custom Context Variables

```
CREATE OR REPLACE CONTEXT DEMO_CTX USING <package>
  ACCESSED GLOBALLY;
```

```
DBMS_SESSION.set_context
     (namespace => DEMO_CTX'
     ,attribute => '…'
     ,value     => '…'
     ,client_id => sys_context('userenv', 'CLIENT_IDENTIFIER')
```

attribute / value is bound to a specific APEX-session

Cleanup:

1. check which sessions are still active (APEX_WORKSPACE_SESSIONS)
2. use dbms_session.clear_context

see also: https://jeffkemponoracle.com/2013/02/apex-and-application-contexts/

SCURTY by Sphinx - Database Security out-of-the-box

Single Point of Control
Security is centrally implemented in the Oracle DB for all applications.

Streamlining the Code
No (potentially inconsistent) implementation of security in different applications.

Client Tool Agnostic
Highly granular row- and column-level security independent of the application.

Centralized Audit
Enables personalized auditing of all database accesses.

100% Metadata Driven
No-code framework that runs directly in the Oracle DB and exclusively utilizes free Oracle EE features.

I have a question.

sphinx

Dr. Thomas Petrik

Sphinx IT Consulting GmbH

T +43 1 599 31 - 0
M +43 664 155 83
thomas.petrik@sphinx.at

Aspernbrückengasse 2
A-1020 Wien

www.sphinx.at

Sphinx & Exasol
auf der DOAG 2024

Besuchen Sie uns an unserem Stand auf Ebene 3!