Virtual Private Database tapasztalatok a Generali Biztosítóban

Csonka Zoltán
Adattárház architekt
csonka.zoltan@generali.com

HOUG Konferencia 2015.

2015.03.27.

Miről lesz szó

- Hogyan találkoztunk a VPD-vel?
- VPD vs. view
- VPD megoldás a Generaliban
- Tapasztalatok

GENERALI

Hogyan találkoztunk VPD-vel

Szigorúan bizalmas adatokat tartalmazó adatkör,
élesítés előtti jogosultság kezelési igény módosítása.

VPD-vel utólagosan is megoldható a jogosultságvédelem,
úgy hogy az erre épülő riportokat, lekérdezéseket nem kell módosítani.

EE környezetben külön licenc díj nélkül használható.
(Ellentétben a Label Security és Database Vault megoldásokkal)

GENERALI

VPD vs. view

View-val is minden megoldható miért kellene VPD?

Nem feltétlenül kell VPD, de gyakran egyszerűbb megoldás.

A VPD biztonságosabb mint a view mert

- a where záradék automatikus kernel szintű hozzáadása - SQL VM -ben.
- View-ban alkalmazott jogkezelés esetében könnyebb megkerülni az alapadatokat
- Védelem séma tulajdonosa ellen és select any table ellen is

VPD policy alkalmazásával bonyolultabb kifejezéseket egyszerűbben lehet összeállítani.

A menedzselés jobban leválasztható a fejlesztéstől. (policy admin user)

RBAC vs. VPD? - RBAC & VPD!

Természetesen a Role alapú, objektumszintű jogosultságvédelem továbbra is marad.

A VPD kiegészíti az RBAC megoldásokat sorszintű, oszlopszintű jogkezeléssel, valamint bonyolultabban megfogalmazható jogosultságkezelési eljárások beépítésével.

GENERALI

Megoldás – Role és Context változó

Sorszintű jogkezelés

- Szerepkörök létrehozása, feltöltése vállalati jogkezelő rendszeren keresztül
  (GP, GP leányvállalat)
- Logon trigger, context változó
  (session létrehozáskor azonosít)

```
CREATE OR REPLACE PACKAGE BODY SYSADMIN_VPD.cla_vallalat_ctx_pkg IS
  PROCEDURE set_cla_vallalat
  AS
    vallalat varchar(20);
  BEGIN
    -- DW_PORTFOLIO
     SELECT granted_role into vallalat
     FROM sys.dba_role_privs
     WHERE grantee = SYS_CONTEXT('USERENV', 'SESSION_USER') and GRANTED_ROLE = 'ALAPKEZELO';

     DBMS_SESSION.SET_CONTEXT('cla_vallalat_ctx', 'alapkezelo', vallalat);

  EXCEPTION
   WHEN NO_DATA_FOUND THEN NULL;
  END set_cla_vallalat;
END;
```


GENERALI

Megoldás – Jogosultság eljárások

Új jogosultság kezelő felhasználó (SYSADMIN_VPD)
Látja a védendő objektumokat és a *dba_role_privs*-t

A policy itt kerül meghatározásra, az eljárok ide kerülnek.

Ezek az eljárások adják meg a where záradékot. Pl.:

```
CREATE OR REPLACE FUNCTION SYSADMIN_VPD.get_dm_portf_bo
  schema_p    IN VARCHAR2,
  table_p     IN VARCHAR2)
 RETURN VARCHAR2
 AS
  vallalat varchar(20);
  pred VARCHAR2 (400);
 BEGIN
        if SYS_CONTEXT('cla_vallalat_ctx', 'alapkezelo
            pred := null;
        else
            pred := 'agazat not in (''PRIVATE BANKING'',''EGYÉB'')';
        end if;

 RETURN pred;
END;
```

```
BEGIN
  SYS.DBMS_RLS.ADD_POLICY     (
    object_schema           => 'REORG_DM'
    ,object_name            => 'DM_PORTF_BONTASA_BEFALAPONKENT'
    ,policy_name            => 'POL_DM_PORTF_BONTASA_BEFALAP'
    ,function_schema        => 'SYSADMIN_VPD'
    ,policy_function        => 'GET_DM_PORTF_BONTASA_BEFALAP'
    ,statement_types        => 'SELECT'
    ,policy_type            => dbms_rls.context_sensitive
    ,long_predicate         => FALSE
    ,update_check           => FALSE
    ,static_policy          => FALSE
    ,enable                 => TRUE );
END;
```


GENERALI

Tapasztalatok

- Nagyon gyorsan és egyszerűen lehetett implementálni!
- Nem volt vele sem munka, sem probléma a bevezetés óta.
- Where záradékba kerül a szűrés, van, hogy megoldható utólag is de előre kellene ezt is tervezni.
- Egyszerűbb, mert a policy függvény újra felhasználható több objektumhoz hozzárendelve adott esetben elég egy helyen elég módosítani.
- Figyelni kell, hogy a policy egyszerű maradjon. Könnyen bonyolítható az eljárás és akkor átláthatatlan lesz.
- A biztonságtechnikai menedzser elégedett.

„Egy tábláról ránézésre nem lehet megállapítani, hogy VPD-vel jogosultságvédett-e.”

GENERALI

Jövőbeli jogosultságkezelés VPD-vel

Mezőszintű jogosultságkezelési igény esetén adatpiaci szinten

Köszönöm a figyelmet!

Várom a kérdéseket!

Csonka Zoltán
Generali Biztosító
Adattárház architekt
csonka.zoltan@generali.com