Adatbázis biztonsági audit és beállítás tapasztalatok

K&H Bank Zrt.

2017.11.08.

Simon Tamás

Tartalom

- Mi az audit, miért csináljuk?
  - Audit típusok
  - Pénzügyi szektor és a K&H
  - Szervezeti sajátosságok
- CIS és PCI DSS
- Audit a K&H Bankban
  - Adatbázis audit alap elvárások
  - Listener poisoning
  - SQL92
  - Központosított jogosultságkezelés
  - 12c privilege capture
  - Unified audit
  - Adatbázisokra ható auditok

Mi az audit, miért csináljuk?

Mi az audit, miért csináljuk?

- Audit, ma már vizsgálat
- Pénzügyi szektor – „agyon auditált” környezet
- Szervezeti felépítés, sajátosságok, IRM
- Audit típusok vizsgáló szerint
  - Belső audit (KBC, K&H)
  - Külső audit (MNB, Hungard, PWC, E&Y)
- Audit típusok vizsgálat tárgya szerint
  - Termékaudit
  - Folyamataudit
  - Rendszeraudit

CIS és PCI DSS

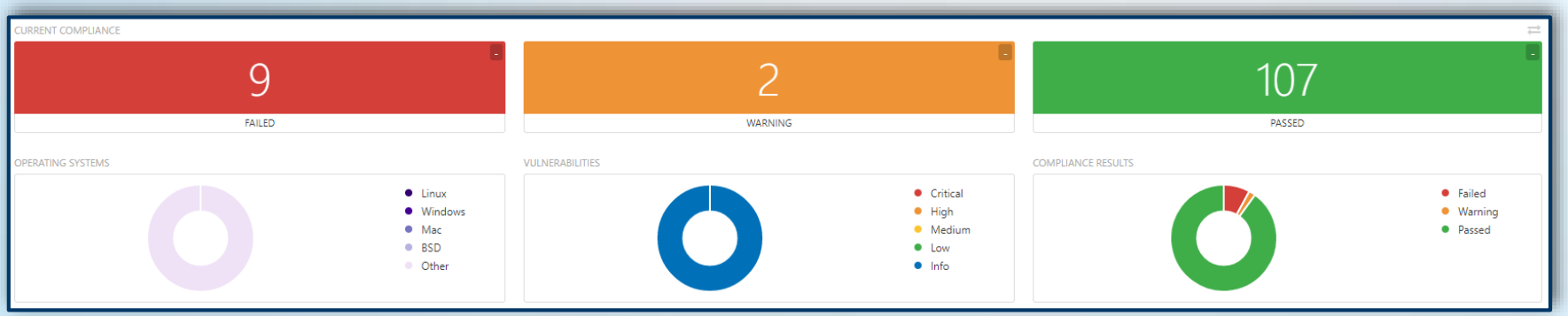
CIS és PCI DSS

- Mi a CIS?
  - Center for Internet Security
  - Célkitűzései
  - Mely platformokra vonatkozik?
- CIS a K&H Bankban
  - Nemzetközi, „group” szintű elfogadók
  - Baseline betartása és betartatása
  - CIS 12c adatbázis alapkonfiguráció
  - Formalizált kivételkezelés
  - Eredmények és értékelések

CIS és PCI DSS

- CIS a K&H Bankban

Sev	Name	Family	Count
●	1.1 Ensure the Appropriate Version/Patches for Oracle Softwar...	Database Compliance Checks	1
●	1.2 Ensure All Default Passwords Are Changed	Database Compliance Checks	1
●	1.3 Ensure All Sample Data And Users Have Been Removed	Database Compliance Checks	1
●	2.2.1 Ensure 'AUDIT_SYS_OPERATIONS' Is Set to 'TRUE'	Database Compliance Checks	1
●	2.2.10 Ensure 'REMOTE_OS_ROLES' Is Set to 'FALSE'	Database Compliance Checks	1



CIS és PCI DSS

- Mi a PCI DSS?
  - Payment Card Industry (PCI) Data Security Standard (DSS) szabvány
  - Kikre vonatkozik a szabályozás?
  - Mi a cél?
  - Szabálysértés esetén komoly büntetések – 500.000$

Audit a K&H Bankban

Audit a K&H Bankban

- Adatbázis audit alap elvárások
  - Központi log gyűjtés (SIEM)
  - audit_trail = OS és a problémák
  - Mi a cél?
  - Kerülő megoldás!

Audit a K&H Bankban

- Megoldás
  - Séma, tábla, procedúra
  - Ütemezett feladat
  - Megfelelő jogosultságok
  - Fájlok generálása
  - RSYSLOG küldi a fájlokat
  - Fogadó fél (SIEM) felkészítése

```
CREATE OR REPLACE procedure sema.valami is
    v_date date;
    v_maxdate date;
    v_dir varchar2(50) := 'directory';
    v_filename varchar2(200) := 'audit_records.log';
    v_file utl_file.file_type;
    v_error varchar2(200);
    v_seqno number;
    cursor cur1 (p_date in date, p_maxdate in date) is
        SELECT TO_CHAR(from_tz(ntimestamp#,'UTC') at time zone 'Europe/Budapest', 'YYYY-MM-DD HH24:MI:SS') ||
        ' '|| HOST_NAME ||
        ' Oracle Audit['|| SESSIONID ||']:' ||
        ' LENGTH : '''|| SESSIONCPU || ''' ||
        ' ACTION:['||TO_CHAR(LENGTH(name)) ||'] ''' || name || ''' ||
        ' DATABASE USER:['||TO_CHAR(LENGTH(USERID)) ||'] ''' || USERID || ''' ||
        ' PRIVILEGE:['||TO_CHAR(LENGTH(SPARE1)) ||'] ''' || SPARE1 || ''' ||
        ' CLIENT USER:['||TO_CHAR(LENGTH(SPARE1)) ||'] ''' || SPARE1 || ''' ||
        ' CLIENT TERMINAL:['||TO_CHAR(LENGTH(TERMINAL)) ||'] ''' || TERMINAL || ''' ||
        ' STATUS:['||TO_CHAR(LENGTH(ACTION#)) ||'] ''' || ACTION# || ''' ||
        ' DBID:['||TO_CHAR(LENGTH(DBID)) ||'] ''' || DBID || ''' as TXT
        FROM sys.v_$instance i, sys.aud$, sys.audit_actions
        WHERE action# = action
        AND from_tz(ntimestamp#,'UTC') at time zone 'Europe/Budapest' > p_maxdate
        and from_tz(ntimestamp#,'UTC') at time zone 'Europe/Budapest' <= p_date;
    v_txt_to_write cur1%rowtype;
    procedure log (p_seqno in number, p_date in date, p_event in varchar2, p_message in varchar2) is
    begin
        insert into sema.tabla values (p_seqno, p_date, p_event, p_message);
        commit;
    end;
```

Audit a K&H Bankban

- Listener poisoning probléma

  - A listener nem végzi el a validációt az adatbázis regisztrációjakor - autentikációt sem követel - így egy támadó, a listener révén a teljes adatbázishoz hozzáfér.

- Megoldás

  - Oracle 11.2.0.4. verzió alatt egyéb patch telepítése is szükséges

  „Patch 12880299: RAC: TCP handlers block if listener registration is restricted to IPC W/COST”

  - Oracle 11.2.0.4. verziótól viszont elég a listener.ora fájl kiegészítése

  „Add the COST TCP protocol restriction "SECURE_REGISTER_[listener_name] = (TCP)" to the listener.ora.”

  - 12c verziótól már javítva

Audit a K&H Bankban

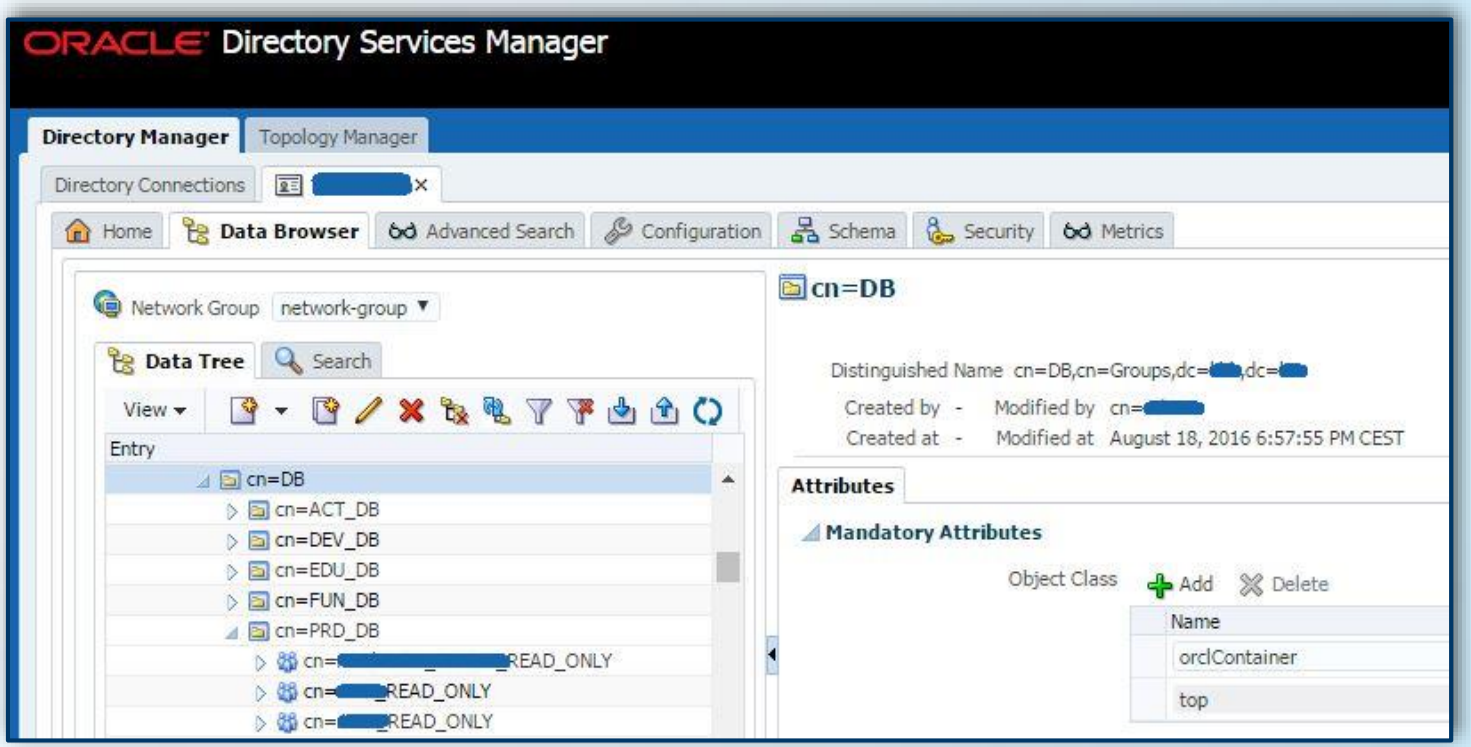
- Az SQL92 paraméter
  - Egyik leggyakoribb ajánlás , default érték FALSE
  - SELECT jog hiányában is adható UPDATE, DELETE jogosultság

```
SQL> grant delete on scott.emp to test;

Grant succeeded.

SQL> show parameter sql92

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------
sql92_security                       boolean     FALSE
SQL> conn test/test
Connected.
SQL> delete from scott.emp where sal>3000;

1 row deleted.

SQL> rollback;

Rollback complete.
```

```
SQL> show parameter sql92

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------
sql92_security                       boolean     TRUE
SQL>
SQL> conn test/test
Connected.
SQL> delete from scott.emp where sal>3000;
delete from scott.emp where sal>3000
                    *
ERROR at line 1:
ORA-01031: insufficient privileges
```

Audit a K&H Bankban

- Központosított jogosultságkezelés
  - Jogosultság kezelő rendszer
  - Igénylések, jóváhagyások itt futnak
  - Auditálható, visszakereshető történések
  - Automatizált szinkronizáció (OUD-EUS)



Audit a K&H Bankban

- 12c Privilege Capture
  - Database Vault opcióban
  - Legkisebb jogosultság elve - Least privilege principle
  - Nehézkes felülvizsgálat
  - Részletesen konfigurálható
  - Jogosultságok riportálhatók

Audit a K&H Bankban

- Unified audit, miért igen?
  - 12c-től egységes keretrendszer
  - Egyszerűsít, egységesít, átláthatóbb
  - Komplex szabályrendszer, Kernel-szintű védelem
  - Integráció (Data Pump, RMAN, SQL Loader, Oracle Label Security)

- Unified audit, miért nem?
  - Konszolidált környezetben performancia problémák
  - Bugok, pl:
    - Audit rekordok nem törlődnek és/vagy nem törölhetők
    - Logon események nem auditálódnak
    - Role-k auditálásával rengetek trace fájl keletkezik

Audit a K&H Bankban

- Adatbázisokra ható más auditok
  - Más rendszereken végrehajtott beállítások
  - Tipikus OS oldali audit beállítás
  - Adatbázis folyamatok nem működtek, ORA-600
  - Megoldás, megfelelő mount opciók használata

```
# cat /etc/fstab
tmpfs /dev/shm  tmpfs  defaults,nodev,nosuid,noexec  0 0

# cat /etc/fstab
tmpfs /dev/shm  tmpfs  defaults,  0 0
```

Kérdések - válaszok

Köszönöm a figyelmet!

tamas.simon@kh.hu

Felhasznált források:

Oracle Security Alert for CVE-2012-1675
Database Vault Administrator's Guide
ORA-600 [pesldl03_MMap: Errno 1 Errmsg Operation Not Permitted] (Doc ID 1625010.1)