AUDIT

ROZDĚLENÍ ODPOVĚDNOSTI

- DBA uživatelé musí být důvěryhodní
  - Zneužití důvěry
  - Audit
- DBA zodpovědnosti mohou být sdílené.
- Účty nesmí být sdílené.
- DBA a administrátor systému by měli být různí lidé.
- Rozdělení práv operátora a administrátora.

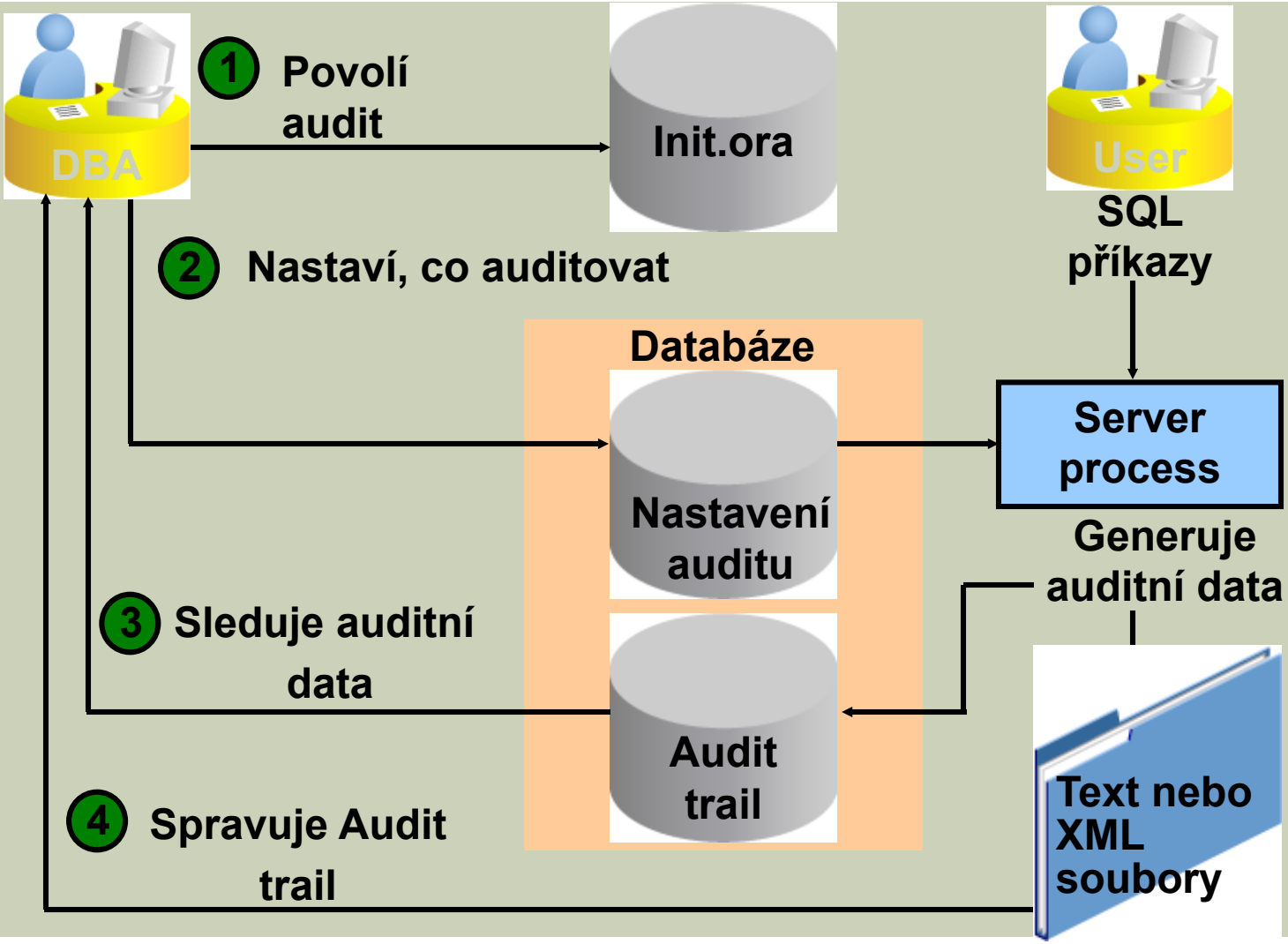
DATABÁZOVÁ BEZPEČNOST

- Poučka - bezpečnost systémů by měla odpovídat důvěrnosti dat v něm obsažených:
  - Restrikce přístupu
  - Autentikace
  - Monitoring

MONITORING

- Monitoring a audit musí být standardní součástí zabezpečení
- Druhy:
  - Základní/Povinný audit – přihlášení AS SYSDBA
  - Standardní databázový audit (dnes často nahrazen unified auditem)
  - Audit změn dat
  - Fine-grained audit (FGA)
  - SYSDBA audit – další operace se oprávněním SYSDBA
  - Unified audit (od verze 12c)

STANDARDNÍ DATABÁZOVÝ AUDIT



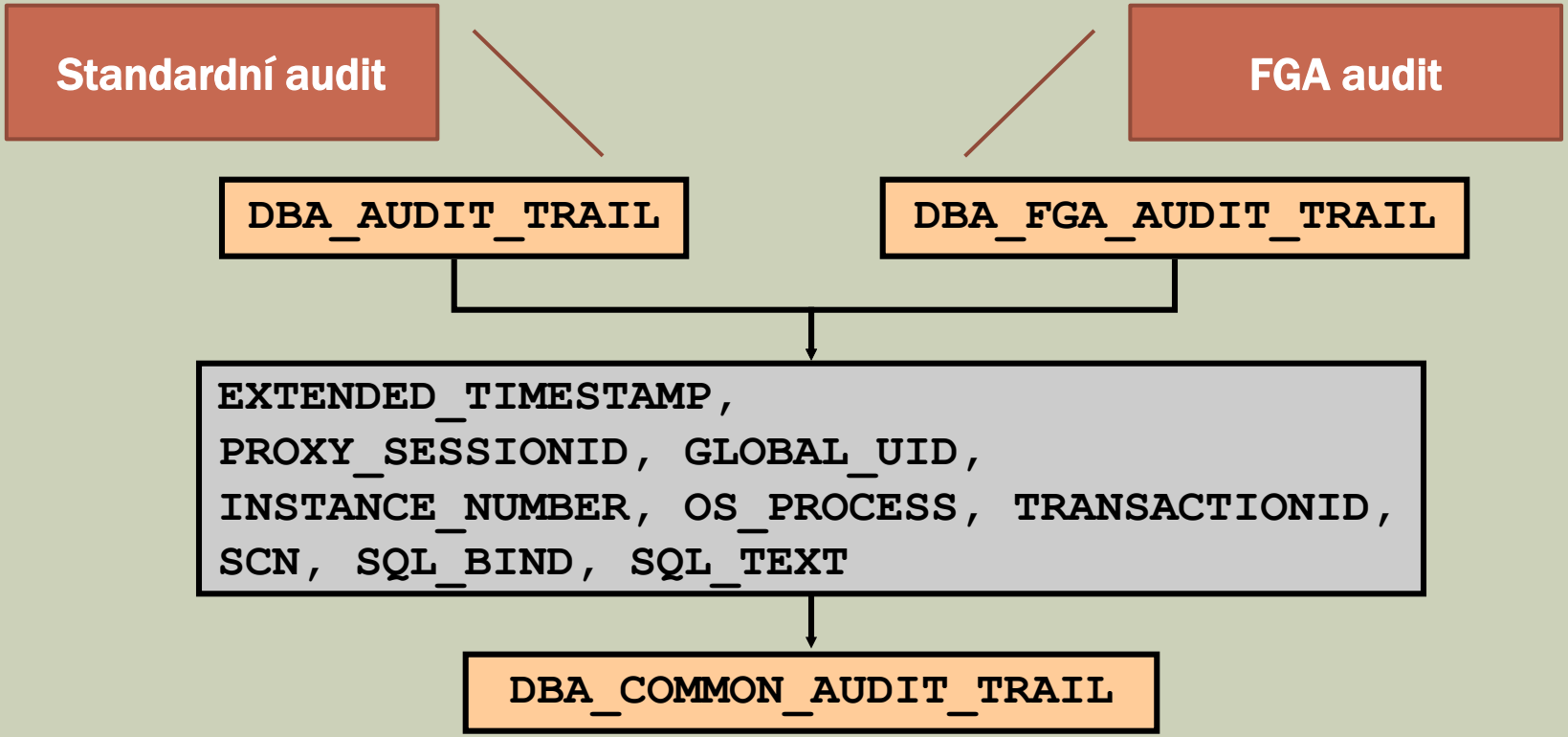
AUDIT TRAIL

- **Audit trail (umístění auditu) se nastavuje inicializačním parametrem** `AUDIT_TRAIL`.
- **Ten může nabývat následujících hodnot:**
  - **NONE**
  - **OS**
  - **DB**
  - **DB, EXTENDED**
  - **XML**
  - **XML, EXTENDED**

```
ALTER SYSTEM SET AUDIT_TRAIL='XML' SCOPE=SPFILE;
```

- Po nastavení parametru je nutný restart databáze !
- Pro úplnbost výčtu - speciálním typem auditu je Unified audit

AUDITNÍ DATA



NASTAVENÍ AUDITU

- **Audit DDL příkazů:**

```
AUDIT table;
AUDIT all by HR;
```

- **Audit systémových práv:**

```
AUDIT select any table, create any trigger;
AUDIT select any table BY hr BY SESSION;
```

- **Audit objektových práv:**

```
AUDIT ALL on hr.employees;
AUDIT UPDATE,DELETE on hr.employees BY ACCESS;
```

NASTAVENÍ AUDITU

- **Audit DML příkazů:**

```
AUDIT UPDATE TABLE, INSERT TABLE, DELETE TABLE, SELECT
TABLE BY HR;
```

- **Audit objektů založených v budoucnosti:**

```
AUDIT UPDATE, INSERT, DELETE, SELECT ON DEFAULT;
```

NASTAVENÍ AUDITU

- **BY ACCESS:**
  - **Default**
  - **Audituje se každá operace**
  - **Více informací (execution time, scn …)**

```
AUDIT select any table BY hr;
```

```
AUDIT select any table BY hr BY ACCESS;
```

- **BY SESSSION**
  - **Stejné operace (např. stejný update) se během připojení audituje jen při první výskytu**
  - **Méně informací**

```
AUDIT select any table BY hr BY SESSION;
```

ZÁKLADNÍ/POVINNÝ AUDIT

- Uživatelé se `SYSDBA` nebo `SYSOPER` právy se mohou přihlásit do databáze i když je zavřená:
  - Audit musí být uchováván mimo databázi
  - Připojení jako `SYSDBA` nebo `SYSOPER` jsou vždy auditována
  - Umístění auditu je dáno parametrem `AUDIT_FILE_DEST`.
  - Pokud adresář neexistuje, nelze se přihlásit
  - NELZE JEJ VYPNOUT!

STANDARDNÍ AUDIT

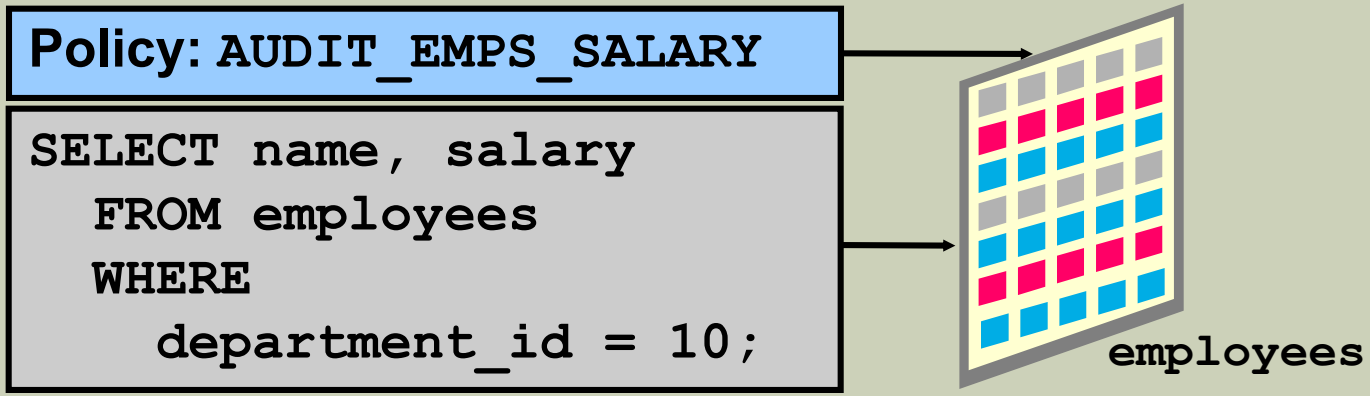
- Defaultně se nic neauditуje
- Pomocí standardního auditu se neauditуje uživatel SYS – má svůj systémový audit, důvodem je, že může pomocí příkazu delete from aud$ stejně všechen audit velice jednoduše smazat
- Zapnutí nebo vypnutí audit zafunguje až pro nově přihlášené uživatele, pro ty již připojené nelze nastavení standardního auditu změnit

AUDIT ZMĚN HODNOT

- Není standardní součástí Oracle databáze
- Řeší se uživatelsky – pomocí tzv. triggerů
- Triggery on insert, on update, on delete … v těle triggeru známe old i new hodnoty, uložíme je do zvláštní tabulky
- Výhody
  - Lze vytvořit audit „na míru“
  - Součástí může být automatický management
  - Součástí může být automatický monitoring
- Nevýhody
  - Vše je psáno v PL/SQL – má nezanedbatelnou režii

FINE-GRAINED AUDIT (FGA)

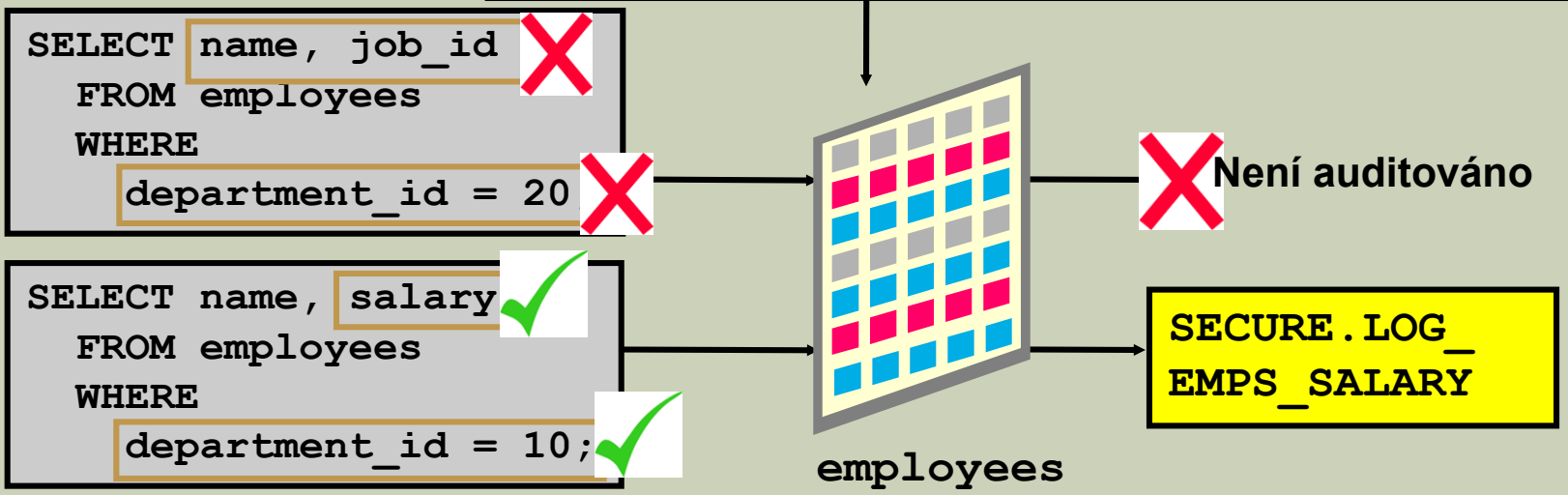
- Monitoruje přístup na základě obsahu
- Audituje `SELECT`, `INSERT`, `UPDATE`, `DELETE` a `MERGE`
- Může být navázán na jeden nebo více sloupečků
- Může spustit proceduru
- Administruje se pomocí `DBMS_FGA` balíku
- Je jen v Enterprise (nejdražší) verzi databáze



FINE-GRAINED AUDIT (FGA)

- Základem je tzv. Policy ta definuje:
  - Kritéria auditu
  - Akce auditu
- Založení pomocí DBMS_FGA .ADD_POLICY

```
dbms_fga.add_policy (
 object_schema   => 'HR',
 object_name     => 'EMPLOYEES',
 policy_name => 'audit_emps_salary',
 audit_condition=>  'department_id=10',
 audit_column    => 'SALARY,COMMISSION_PCT',
 handler_schema  => 'secure',
 handler_module  => 'log_emps_salary',
 enable          => TRUE,
 statement_types => 'SELECT,UPDATE');
```

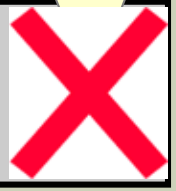


FINE-GRAINED AUDIT (FGA)

- Jsou auditovány pouze záznamy, které odpovídají FGA predikátu (podmínce) a vztahují se k danému sloupečku
- `DELETE` příkazy jsou auditovány bez ohledu na sloupeček
- `MERGE` příkazy jsou auditovány tak, jakoby to byly vlastně jednotlivé `INSERT`, `UPDATE` a `DELETE` příkazy

Není auditováno protože žádný měněný řádek není pro department=10

```
UPDATE hr.employees
SET salary = 1000
WHERE commission_pct = .2;
```



```
UPDATE hr.employees
SET salary = 1000
WHERE employee_id = 200;
```

FINE-GRAINED AUDIT (FGA)

- Pro audit všech řádek použijeme `null` podmínku
- Pro audit všech sloupečků použijeme `null` pro specifikaci sloupečku
- Pojmenování jednotlivých Policy je unikátní
- Auditovaná tabulka nebo pohled musí existovat ve chvíli, kdy Policy vytváříme
- Pokud je podmínka auditu chybná, uživateli se při přístupu k datům objeví `ORA-28112` error a přístup mu není umožněn
- Pokud auditovaný sloupeček není v dané tabulce, nejsou auditovány žádné řádky
- Pokud neexistuje volaná procedura, nedojde k chybě a audit zafunguje

SYSDBA AUDIT

- Zapíná se parametrem AUDIT_SYS_OPERATIONS
- Audituje uživatele se SYSDBA nebo SYSOPER právy
- Umístění auditu je dáno parametrem AUDIT_FILE_DEST.
- Audituje všechny top-level příkazy, tj. při spuštění procedury audituje pouze vlastní spuštění, nikoliv už příkazy, které se vykonávají v rámci procedury

SPRÁVA AUDITNÍCH DAT

- Best-practices:
  - Data průběžně monitorujeme
  - Hlídáme velikost
  - Zálohujeme
- Od verze 11g systémová package DBMS_AUDIT_MGMT
  - DBMS_AUDIT_MGMT.set_audit_trail_location – přesun auditu
  - DBMS_AUDIT_MGMT.clear_audit_trail_property – kdy a jak mazat auditní data
  - DBMS_AUDIT_MGMT.clean_audit_trail – maže auditní data dle nastavení
  - DBMS_AUDIT_MGMT.create_purge_job – vytvoří job, který audit pravidelně promazává

UNIFIED AUDIT

- K dispozici od 12c
- Speciální uživatel AUDSYS
- Speciální read only tabulka UNIFIED_AUDIT_TRAIL, kterou nelze nijak modifikovat
  Audit se zapíná na úrovni OS přelinkováním knihoven oracle (při vypnuté databázi)

```
$ cd $ORACLE_HOME/rdbms/lib
$ make -f ins_rdbms.mk uniaud_on ioracle
```

- Vypnutí stejně jen s parametrem uniaudit_off
- Zda je unified audit nastaven, zjistíme následujícím selektem

```
SQL>select parameter,value from v$option where parameter
= 'Unified Auditing';
```

- Speciální role AUDIT_ADMIN a AUDIT_VIEW
- Pokud jej zapneme, automaticky se vypne původní **standard audit**
- **FGA audit** funguje stále, jen je ukládán do UNIFIED_AUDIT_TRAL

UNIFIED AUDIT – LADĚNÍ VÝKONU

- Okamžitý zápis (stejně jako u ostatních typů auditu)

```
EXECUTE DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_PROPERTY(-
 DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED, -
 DBMS_AUDIT_MGMT.AUDIT_TRAIL_WRITE_MODE, -
 DBMS_AUDIT_MGMT.AUDIT_TRAIL_IMMEDIATE_WRITE);
```

- Zápis pomocí fronty

```
EXECUTE DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_PROPERTY(-
 DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED, -
 DBMS_AUDIT_MGMT.AUDIT_TRAIL_WRITE_MODE, -
 DBMS_AUDIT_MGMT.AUDIT_TRAIL_QUEUED_WRITE);
```

- Velikost fronty lze nastavit inicializačním parametrem *unified_audit_sga_queue_size*
- Pokud není fronta prázdná a databáze „spadne“, pak se auditní data z fronty nenávratně ztratí

UNIFIED AUDIT

- Povinně se pomocí unified auditu audituje:
  - CREATE AUDIT POLICY
  - ALTER AUDIT POLICY
  - DROP AUDIT POLICY
  - AUDIT
  - NOAUDIT
  - EXECUTE of the DBMS_FGA PL/SQL package
  - EXECUTE of the DBMS_AUDIT_MGMT PL/SQL package
  - ALTER TABLE attempts on the AUDSYS audit trail table
  - Top level statements by the administrative users SYS, SYSDBA, SYSOPER, SYSASM, SYSBACKUP, SYSDG, and SYSKM

UNIFIED AUDIT

- Co chci auditovat, můžu sdružit do tzv. policies

```
CREATE AUDIT POLICY os_users_priv_pol
PRIVILEGES SELECT ANY TABLE, CREATE TABLE
WHEN 'SYS_CONTEXT (''USERENV'', ''OS_USER'') IN
(''psmith'', ''jrawlins'')' EVALUATE PER
SESSION/STATEMENT;

AUDIT POLICY os_users_priv_pol;
```

```
CREATE AUDIT POLICY all_actions_on_hr_emp_pol
 ACTIONS ALL ON HR.EMPLOYEES;

AUDIT POLICY all_actions_on_hr_emp_pol EXCEPT pmulligan;
```

UNIFIED AUDIT

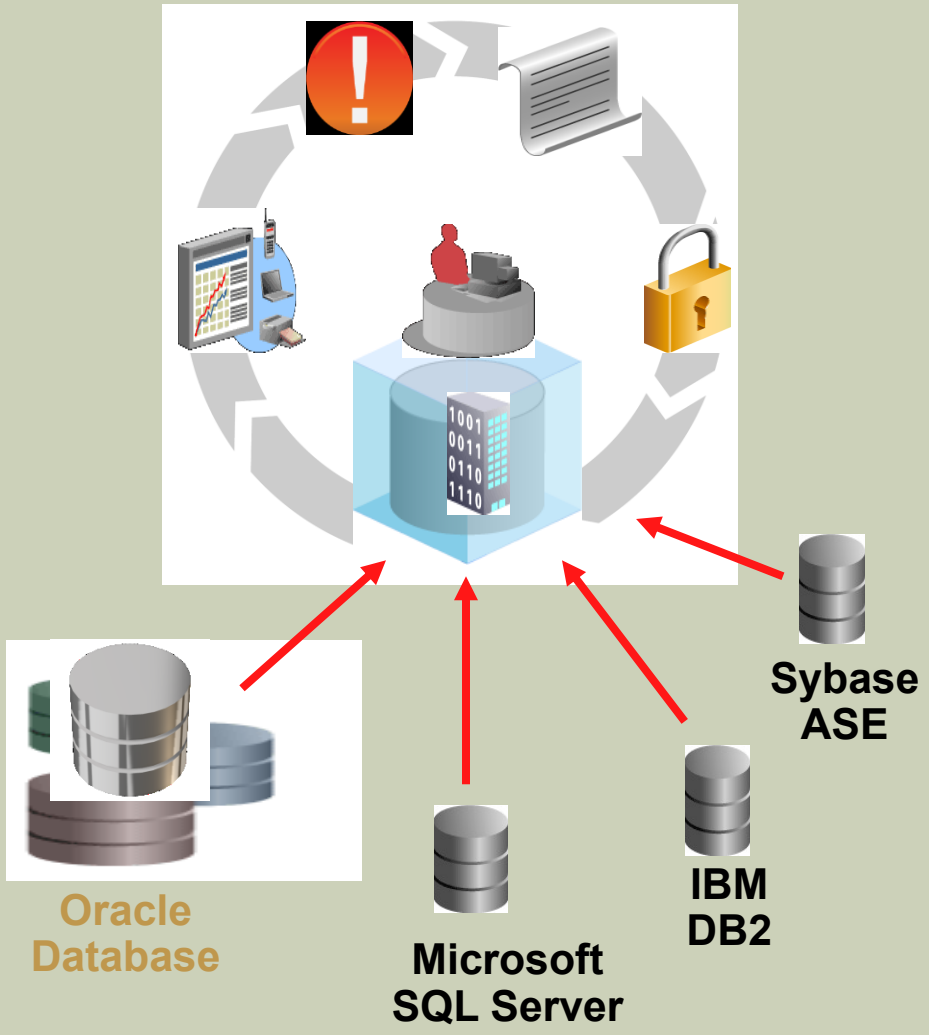
- Audit DML

```
create audit policy test_audit_policy1
  actions delete on test.tab1, insert on test.tab1,
          update on test.tab1, select on test.tab1,
          all on test.tab2, select on test.tab3
  when 'sys_context(''userenv'',''session_user'') = 'TEST'''
  evaluate per session;

AUDIT POLICY test_audit_policy1;
```

```
create audit policy test_audit_policy2
  actions delete, insert, update, select
  when 'sys_context(''userenv'',''session_user'') ='TEST'''
  evaluate per session;

AUDIT POLICY test_audit_policy2;
```

ZPRACOVÁNÍ AUDITU - ORACLE AUDIT VAULT

- Consolidate and secure audit data
  - Oracle
  - SQL Server
  - IBM DB2
  - Sybase
  - Secure and scalable
  - Cleanup of source Oracle audit data
- Centralized reporting
  - Updated reports interface using widely popular Oracle Application Express
  - Standard reports for compliance
  - New custom reports
- Alert on security threats
  - Detect and alert on security relevant events



DOTAZY?