ORDIX AG

Auditing
Sinn, Einsatzmöglichkeiten und Performance

Webinar „Auditing“
Klaus Reimers
Leiter Beratung
09.11.2012, Paderborn

kr@ordix.de
www.ordix.de

Agenda

ORDIX AG

- Sinn und Zweck des Auditing
- Methoden und Einsatzmöglichkeiten
  - mit Demos
- Performancebetrachtung
  - mit Demos

Sinn des Auditing - Fragestellungen

ORDIX AG

Klassische Kundenanforderungen:

- Wer ändert Inhalte sensibler Tabellen?
- Wer verändert die Struktur von Tabellen?
- Wer greift mit welchen Rechten zu?
- Wer liest Kontodaten aus?
- Was macht der Benutzer REIMERS?
- Wer versucht, sich in die Datenbank zu hacken?
- ...

Agenda

ORDIX AG

- Sinn und Zweck des Auditing
- Methoden und Einsatzmöglichkeiten
  - mit Demos
- Performancebetrachtung
  - mit Demos

Auditing - Überblick

ORDIX AG

4 Grundformen des Auditing:

- Mandatory Auditing
- SYS Auditing
- Standard Auditing
- Fine Grained Auditing (FGA)

Mandatory Auditing

ORDIX AG

Überwachung von:

- Startup
- Shutdown
- Zugriff mit SYSDBA oder SYSOPER

Automatische Speicherung

- UNIX: $ORACLE_HOME/rdbms/audit
  - modifizierbar über init.ora Parameter: audit_file_dest
- Microsoft: Ereignisanzeige

Mandatory Auditing - Unix -

ORDIX AG

```
Audit file /oracle/product/10g/rdbms/audit/ora_22195.aud
Oracle Database 10g Enterprise Edition Release 10.1.0.3.0 - Production
With the Partitioning, OLAP and Data Mining options
ORACLE_HOME = /oracle/product/10g
System name:    Linux
Node name:      trainix
Release:        2.6.5-7.97-smp
Version:        #1 SMP Fri Jul 2 14:21:59 UTC 2004
Machine:        i686
Instance name: ora00
Redo thread mounted by this instance: 1
Oracle process number: 10
Unix process pid: 22195, image: oracle@trainix (TNS V1-V3)

Tue Aug 30 17:19:51 2005
ACTION : 'CONNECT'
DATABASE USER: '/'
PRIVILEGE : SYSDBA
CLIENT USER: ora00
CLIENT TERMINAL: pts/0
STATUS: 0
```

Mandatory Auditing

ORDIX AG

Überwachung von:

- Startup
- Shutdown
- Zugriff mit SYSDBA oder SYSOPER

Automatische Speicherung

- UNIX: $ORACLE_HOME/rdbms/audit
  - modifizierbar über init.ora Parameter: audit_file_dest
- Microsoft: Ereignisanzeige

Mandatory Auditing - Microsoft -

ORDIX AG

SYS Auditing

ORDIX AG

- Überwachung aller Aktionen des Users SYS
  - auch bei Anmeldung über SYSDBA oder SYSOPER
- Aktivierbar über init.ora Parameter

  AUDIT_SYS_OPERATIONS (statisch)
  - true aktiviert
  - false deaktiviert
- Speicherung
  - UNIX: $ORACLE_HOME/rdbms/audit
    - modifizierbar über init.ora Parameter: audit_file_dest
  - Microsoft: Ereignisanzeige

Standard Auditing - Aktivierung -

ORDIX AG

- Aktivierbar über init.ora Parameter
  - AUDIT_TRAIL (statisch)

none/false	Deaktiviert
os	Speicherung auf Betriebssystemebene
db / true	Speicherung in der Datenbank (SYS.AUD$)
db_extended	Zusätzliche Speicherung von SQL-Text und Bind-Variablen
xml /xml_extended	Speicherung im XML Format im Filesystem

Standard Auditing - Möglichkeiten -

ORDIX AG

- Auditing auf Tabellen und Views
- Auditing auf Aufruf von Prozeduren
- Auditing von Nutzung besonderer Systemprivilegien, wie z.B.
  - DISABLE TRIGGER
  - Nutzung des ANY Privilegs
- Auditing auf erfolgreiche / erfolglose Durchführung einer Aktion
- Beschränkung auf definierte Benutzer
- Möglichkeit der Definition jedes Zugriffs (BY ACCESS) oder einmalig (BY SESSION)

Standard Auditing – Beispiele (I)-

ORDIX AG

- DDL Statements:
  - z. B.: AUDIT TABLE;

    → Protokolliert CREATE, DROP und TRUNCATE auf alle Tabellen

- DML Statements
  - z. B.: AUDIT SELECT TABLE;

    → Protokolliert alle lesenden Zugriffe auf alle Tabellen

Standard Auditing – Beispiele (II)-

ORDIX AG

- Auditing nur für bestimmte Benutzer aktiviert
  - z. B.: AUDIT DELETE TABLE BY KR;

    → Alle löschenden Zugriffe des Users KR werden protokolliert.

- Auditing nur erfolgreicher/erfolgloser Aktionen
  - z. B.: AUDIT ROLE WHENEVER SUCCESSFUL;

    AUDIT ROLE WHENEVER NOT SUCCESSFUL;

    → Alle erfolgreichen/erfolglosen DDL-Statements auf Roles werden protokolliert.

Views

ORDIX AG

DBA_STMT_AUDIT_OPTS	aktivierte Audit Options auf Statement-Ebene
DBA_PRIV_AUDIT_OPTS	aktivierte Audit Options auf Privilegien-Ebene
DBA_AUDIT_TRAIL	alle Audit-Einträge
DBA_AUDIT_SESSION	per CONNECT oder DISCONNECT ausgelöst
DBA_AUDIT_STATEMENT	per AUDIT, NOAUDIT, GRANT, REVOKE, ALTER SYSTEM ausgelöst
DBA_AUDIT_OBJECT	objektbezogene Einträge
DBA_AUDIT_EXISTS	per AUDIT EXISTS oder AUDIT NOEXISTS ausgelöst

Fine Grained Auditing

ORDIX AG

Erweiterung der Auditing-Möglichkeiten durch FGA:

- DML- und SELECT-Statements mitschneiden
- Monitoring des Datenzugriffs basierend auf dem Inhalt
- Kann wie ein SELECT-Trigger wirken

FGA Policy erstellen

ORDIX AG

Beispiel:

- Audit aufsetzten für jeden, der ein SELECT gegen eine bestimmte Tabelle ausführt,
  → FGA-Policy für die Tabelle
- Voraussetzung:
  Privileg execute für das Package **dbms_fga**

```
begin
dbms_fga.add_policy (
        object_schema=>,test',
   object_name=>'mitarbeiter',
        policy_name=>'mitarbeiter_zugriff'  );
end;
```

FGA Policy erstellen

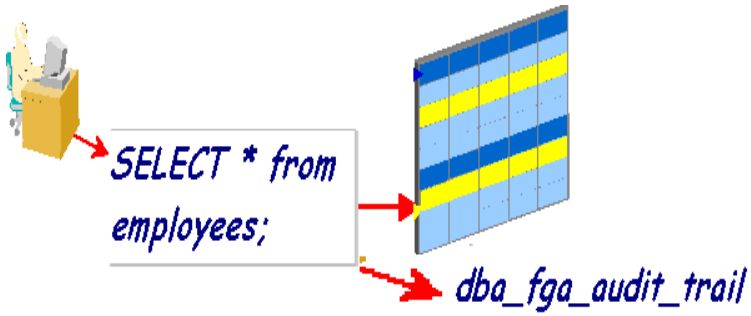
ORDIX AG

Auswirkung der Policy:

- Jedes SELECT gegen die Tabelle wird in einer internen Tabelle protokolliert.
- View **dba_fga_audit_trail**

```
SELECT * from mitarbeiter;

select
    timestamp,
    db_user,
    os_user,
    object_schema,
    object_name,
    sql_text
from
    dba_fga_audit_trail
```



FGA Data Dictionary Views

ORDIX AG

FGA Data Dictionary Views:

- Die vom Audit erstellten Datensätze werden in FGA_LOG$ (gehört SYS) gespeichert. Die Informationen werden in einigen Views zur Verfügung gestellt, z.B. **DBA_FGA_AUDIT_TRAIL**.
- Die Definition einer FGA Policy kann über die View **DBA_AUDIT_POLICIES** eingesehen werden

```
Select * from dba_audit_policies;

Select * from dba_fga_audit_trail;
```

Audit Columns

ORDIX AG

Das Audit wird fokussiert auf Spalten

→ Durch Angabe einer Audit Column werden nur Angaben zu SELECTs gespeichert, die auf eine bestimmte Spalte zugreifen.

```
begin
dbms_fga.add_policy (
        object_schema=>,test',
   object_name=>'mitarbeiter',

        policy_name=>'mitarbeiter_zugri
   ff',
        audit_column => 'gehalt'  );
end;
```

Audit Conditions

ORDIX AG

Das Audit weiter fokussieren auf Bedingungen auf Spalten

→ Durch Angabe einer Audit Condition werden nur Angaben zu SELECTs gespeichert, die auf eine bestimmte Spalte zugreifen und eine bestimmte Bedingung erfüllen.

```
begin
dbms_fga.add_policy (
        object_schema=>,test',
   object_name=>'mitarbeiter',

        policy_name=>'mitarbeiter_zugri
   ff',
        audit_condition => 'gehalt >=
   50000'  );
end;
```

„Reichweite“ der FGA Policies

ORDIX AG

Oracle9*i*

- SELECT-Statements

ORACLE 10g

- zusätzlich DML-Statements
  - INSERT
  - UPDATE
  - DELETE

FGA und Views

ORDIX AG

FGA Policy wirkt auch bei Abfragen über Views:

- Auch der Zugriff auf die Tabelle über eine View fällt unter das Audit und wird gespeichert.
- Aufgeführt wird diese Abfrage unter dem **`object_name`** der Tabelle

Eine FGA Policy kann auch speziell für eine View erstellt werden:

- Für eine View wird eine eigene Policy erstellt.
- Die Abfrage der View erscheint dann unter dem eigenen **`object_name`** der View.

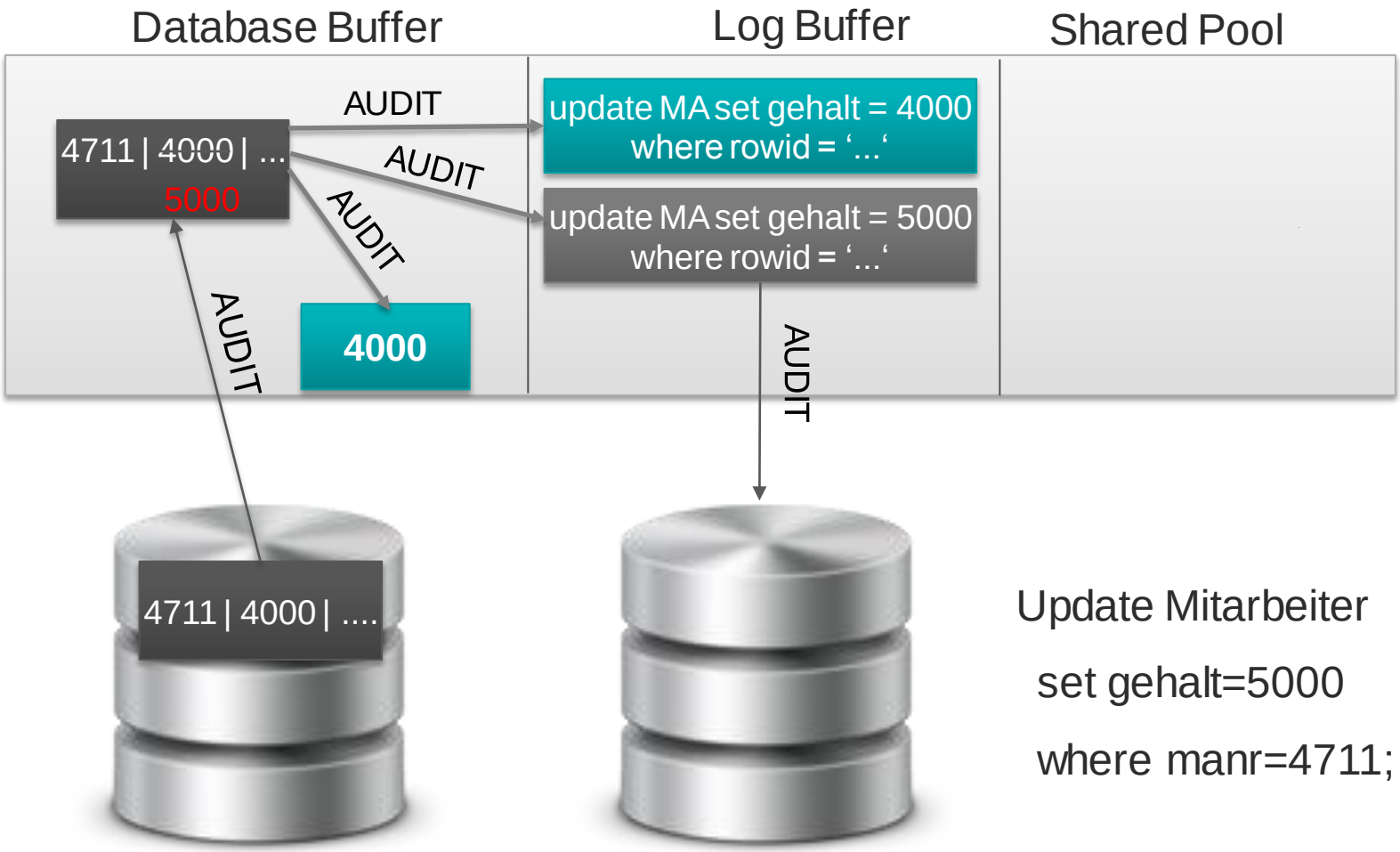
Agenda

ORDIX AG

- Sinn und Zweck des Auditing
- Methoden und Einsatzmöglichkeiten
  - mit Demos
- Performancebetrachtung
  - mit Demos

Beispieltransaktion - Demonstration

ORDIX AG



Update Mitarbeiter

set gehalt=5000

where manr=4711;

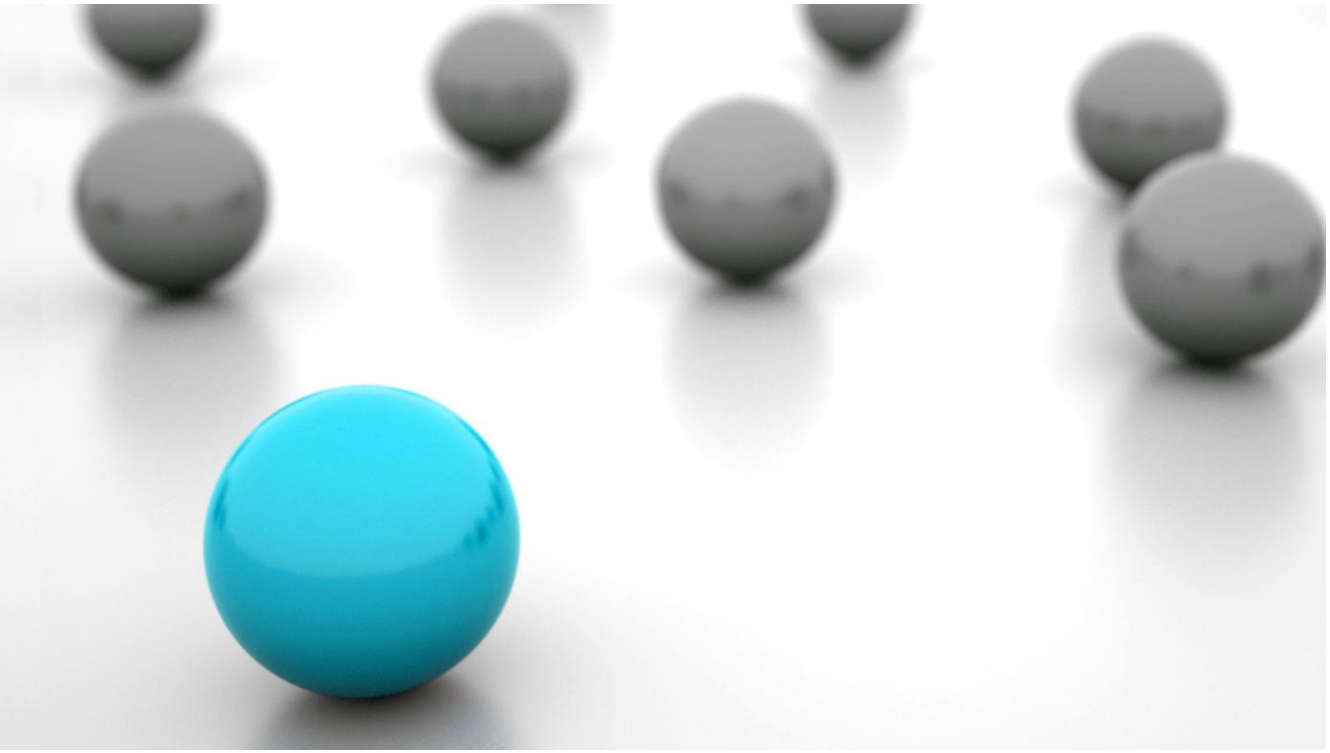
Performance - Einflüsse

ORDIX AG

- UNDO TABLESPACE
  - UNDO Segmente
  - UNDO_RETENTION
    - DBWR + Leseprozesse haben höhere Last
- Log Buffer
  - UNDO Statement
  - REDO Statement
    - LGWR hat höhere Last
    - ARCH hat höhere Last
- Flashback Area
  - DB_FLASHBACK_RETENTION_TARGET
    - RVWR hat höhere Last
- RMAN - inkrementelle Sicherungen
  - Block Change Tracking

Wenn das System „LUFT“ hat, kann man AUDITING nutzen!

ORDIX AG



Zentrale Paderborn
Westernmauer 12 - 16
33098 Paderborn
Tel.: 05251 1063-0

Seminarzentrum Wiesbaden
Kreuzberger Ring 13
65205 Wiesbaden
Tel.: 0611 77840-00

Zentrales Fax:
0180 1 67349 0
0180 1 ORDIX 0

Weitere Geschäftsstellen
in Köln, Münster und Neu-Ulm

E-Mail: info@ordix.de
Internet: http://www.ordix.de

Vielen Dank für Ihre Aufmerksamkeit!