DOAG Regionaltreffen

# Unified Database Auditing

Marco Mischke – 14.05.2019



ORACLE Platinum Partner

robotron®

# Wer bin ich

Oracle DBA since 2000 and Version 7.3.4

Certified Professional 10g, 11g

RAC / Cluster Certified Expert 10g, 11g, 12c

Oracle ACE

@DBAMarco

dbamarco.wordpress.com

ORACLE Certified Professional
Oracle Database 11g Administrator

ORACLE Certified Expert
Oracle Database 12c: Oracle RAC and Oracle Grid Infrastructure Administrator

# Agenda

| | |
|---|---|
| 1 | ▸ Warum Auditing |
| 2 | ▸ Die Welt vor 12.1 |
| 3 | ▸ Unified Auditing ab 12.1 |
| 4 | ▸ Erstellen und Umsetzen von Audit Konzepten |
| 5 | ▸ Auswerten von Audit Daten |
| 6 | ▸ Housekeeping |

# Warum Auditing?

# Warum Auditing?

## Sicherheit in der IT

### Berechtigungen verwalten

- Einschränken der Möglichkeiten
- **WER** darf **WAS**
- Least Privileges Principle
  - So wenig wie möglich
  - So viel wie nötig

- Schaden im Vorfeld vermeiden

# Warum Auditing?

## Sicherheit in der IT

### Berechtigungen verwalten

- Einschränken der Möglichkeiten
- **WER** darf **WAS**
- Least Privileges Principle
  - So wenig wie möglich
  - So viel wie nötig
- Schaden im Vorfeld vermeiden

### Berechtigungen überwachen

- Überwachen der Möglichkeiten
- **WER** hat **WANN WAS** gemacht
- Nachvollziehbarkeit von Aktivitäten
- Angriffe erkennen und (nachträglich) analysieren

# Warum Auditing?

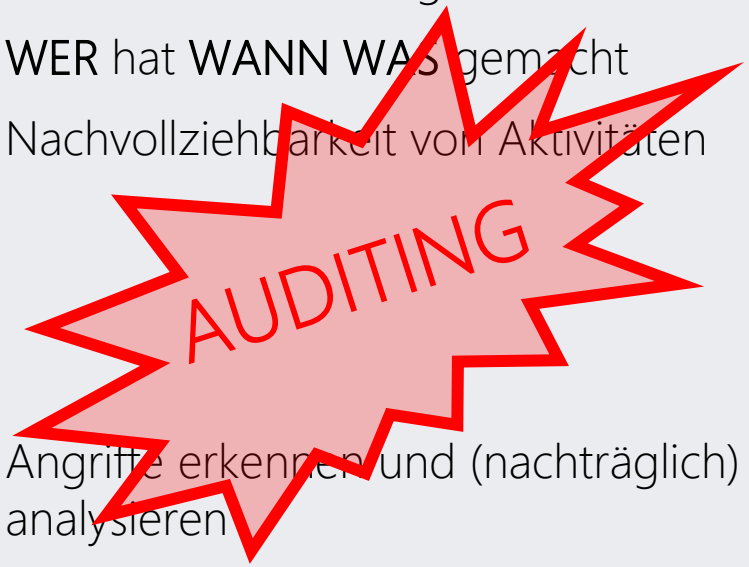
## Sicherheit in der IT

### Berechtigungen verwalten

- Einschränken der Möglichkeiten
- **WER** darf **WAS**
- Least Privileges Principle
  - So wenig wie möglich
  - So viel wie nötig
- Schaden im Vorfeld vermeiden

### Berechtigungen überwachen

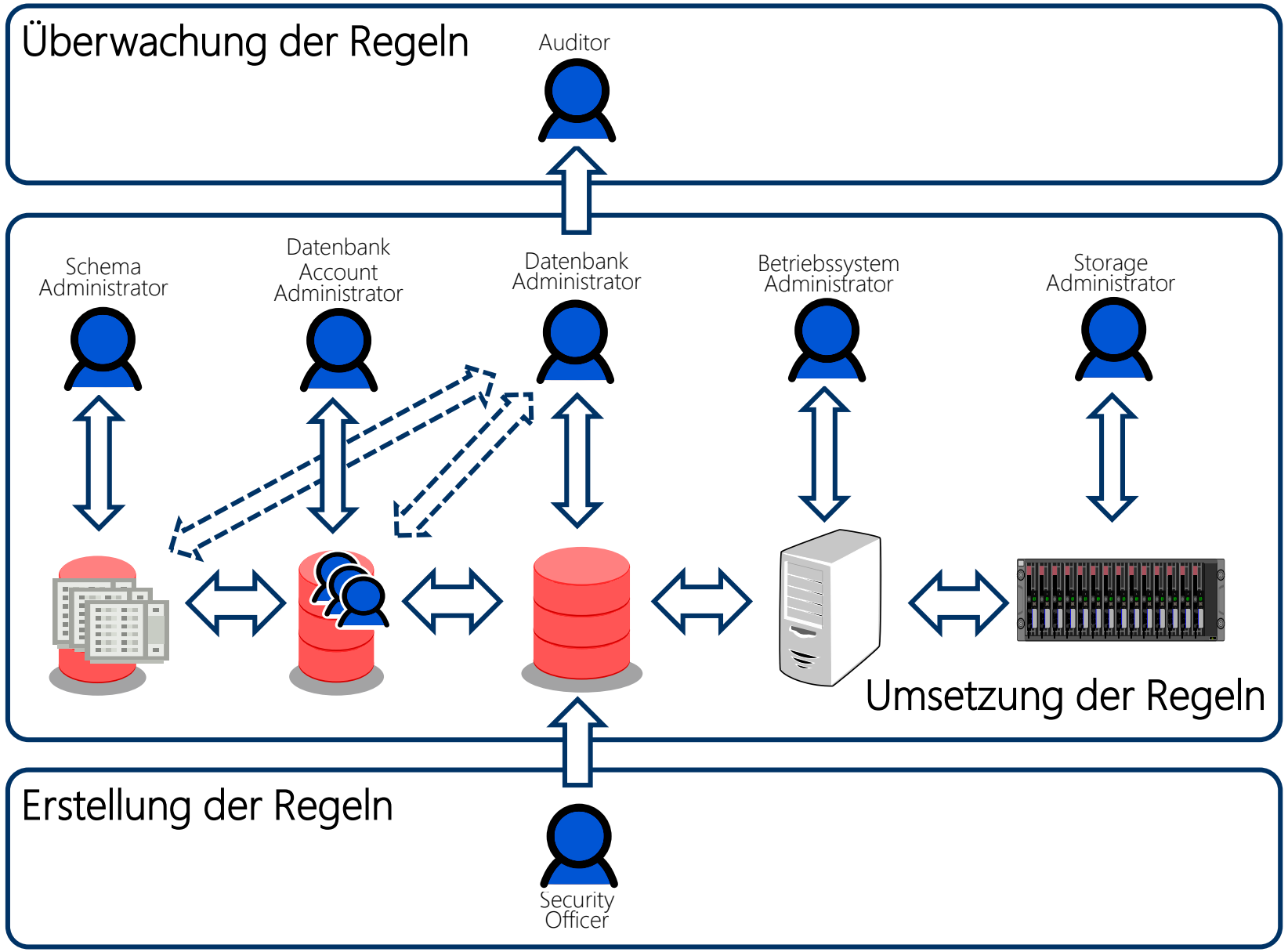
- Überwachen der Möglichkeiten
- **WER** hat **WANN WAS** gemacht
- Nachvollziehbarkeit von Aktivitäten




- Angriffe erkennen und (nachträglich) analysieren

# Warum Auditing

## Separation of Duties



# Die Welt vor 12.1

# Die Welt vor 12.1

## Legacy Auditing

- Verschiedene Audit Möglichkeiten
  - Database Auditing (AUDIT | NOAUDIT)
    - Überwachen von Berechtigungen, Objekten, SQL und Netzwerk
    - SYS.AUD$
  - Fine Grained Auditing
    - Überwachung auf Datensatzebene
    - SYS.FGA_LOG$
  - SYS Auditing
    - Überwachung der SYSDBA Aktivitäten
    - Files in audit_file_dest

# Die Welt vor 12.1

## Legacy Auditing

- Standard Auditing - Initialisierungsparameter
  - AUDIT_TRAIL
    - DB — Daten werden in der Datenbank gespeichert (AUD$)
    - DB,EXTENDED — Wie DB, nur zusätzlich mit dem verursachenden SQL + Bind Variablen
    - OS — Daten werden im Betriebssystem als Datei abgelegt (AUDIT_FILE_DEST)
    - XML — Wie OS, nur im XML-Format
    - XML,EXTENDED — Wie XML, nur zusätzlich mit dem verursachenden SQL + Bind Variablen
    - NONE — Kein Auditing
  - AUDIT_SYS_OPERATIONS
    - TRUE — Alle Aktivitäten mit SYSDBA | SYSOPER Privilegien werden überwacht wird immer nach AUDIT_FILE_DEST geschrieben

# Die Welt vor 12.1

## Legacy Auditing

- Einschränkungen des Legacy Auditing
  - SYS darf das Datenbank Audit Trail ändern
    - UPDATE, DELETE, TRUNCATE der Tabelle SYS.AUD$
  - Entkopplung von SYS nur mit AUDIT_TRAIL = OS | XML
    - Die Dateien können auf OS Ebene vor Veränderung geschützt werden
  - SYS kann die Audit Regeln nach Belieben verändern
  - Audit Regel werden direkt für alle Datenbanknutzer oder eine Liste von Nutzern (de)aktiviert
    - Keine Gruppierung möglich (vgl. Rollen zur Vergabe von Privilegien)

# Die Welt vor 12.1

## Legacy Auditing

- Beispiele
  - SQL Statement Auditing
    - `AUDIT DELETE TABLE BY ACCESS WHENEVER NOT SUCCESSFUL;`
  - Privilege Auditing
    - `AUDIT DROP USER BY ACCTMGR;`
  - Object Auditing
    - `AUDIT SELECT,INSERT,UPDATE,DELETE ON HR.EMPLOYEES WHENEVER SUCCESSFUL;`
    - `AUDIT EXECUTE ON DIRECTORY EXTPROCDIR BY ACCESS;`
  - Network Auditing
    - `AUDIT NETWORK BY ACCESS;`

# Unified Auditing ab 12.1

# Unified Auditing ab 12.1

## Die neue Welt

- Einer für Alle – Unified Auditing
  - Alle Audit Logs werden zusammengeführt
  - SYS kann das Audit Log in der Datenbank nicht mehr verändern
  - Einführung von Audit Policies, Gruppierung von Audit Einstellungen (vgl. Rollen)
  - Separation of Duties
  - Keine Dateien mehr im Betriebssystem
    - Naja, fast…
  - Bedingte Auditierung
  - Auditierung nach Komponenten

```
select COMPONENT, NAME from auditable_system_actions order by 1,2;
```

# Unified Auditing ab 12.1

## Die neue Welt

- Zwei Modi: Mixed und Unified

- Aktivierung des puren Unified Auditing
  - Datenbank(en) anhalten
  - cd $ORACLE_HOME/rdbms/lib
    make -f ins_rdbms.mk uniaud_on ioracle
  - Datenbank(en) starten
- Separaten Tablespace verwenden
- Policies anlegen
- Policies den entsprechenden Nutzern zuweisen

# Erstellen und Umsetzen von Audit Konzepten

# Erstellen und Umsetzen von Audit Konzepten

## Vorbereitung

- Auditing
  - ersetzt nicht ein ausgereiftes Berechtigungskonzept
  - ermöglicht eine nachträgliche Analyse
  - kann ein Mittel zur Früherkennung sein

# Erstellen und Umsetzen von Audit Konzepten

## Vorbereitung

- Zielstellung: **Was** soll auditiert werden und **warum**?
  - WAS:
    - Welche Berechtigungen können Schaden verursachen
    - Welche Benutzer können Schaden verursachen
    - Welche Daten sind besonders gefährdet bzw. schützenswert?
  - WARUM:
    - Was sind möglichen Risiken?
    - Welcher Schaden kann angerichtet werden?

# Erstellen und Umsetzen von Audit Konzepten

## Vorbereitung

- Generelle Aktivitäten
  - SYS Operationen
  - Änderungen am System → ALTER DATABASE, ALTER SYSTEM
  - Änderungen an Benutzern / Rollen → CREATE, ALTER, DROP USER, ROLE
  - Änderungen an Berechtigungen → GRANT, REVOKE
  - Änderungen am Auditing → AUDIT, NOAUDIT
  - Anmeldungen am System → Erfolgreich und/oder Nicht Erfolgreich
  - Änderungen an Wallets → ADMINISTER KEY MANAGEMENT
  - Alle ANY Privilegien
- Applikationsspezifische Aktivitäten
  - Änderungen an (gefährdeten/kritischen) Objekten
  - Zugriffe und/oder Änderungen auf/an gefährdete Daten

# Erstellen und Umsetzen von Audit Konzepten

## Vorbereitung

- Generelle Aktivitäten
  - SYS Operationen
  - Änderungen am System → ALTER DATABASE, ALTER SYSTEM
  - Änderungen an Benutzern / Rollen → CREATE, ALTER, DROP USER, ROLE
  - Änderungen an Berechtigungen → GRANT, REVOKE
  - Änderungen am Auditing → AUDIT, NOAUDIT
  - Anmeldungen am System → Erfolgreich und/oder Nicht Erfolgreich
  - Änderungen an Wallets → ADMINISTER KEY MANAGEMENT
  - Alle ANY Privilegien
- Applikationsspezifische Aktivitäten
  - Änderungen an (gefährdeten/kritischen) Objekten
  - Zugriffe und/oder Änderungen auf/an gefährdete Daten

# Erstellen und Umsetzen von Audit Konzepten

## Vorbereitung

1. Herkömmliches Auditing deaktivieren

```
NOAUDIT ALL;
```

2. Standard Policies deaktivieren

```
NOAUDIT POLICY ORA_SECURECONFIG;
NOAUDIT POLICY ORA_LOGON_FAILURES;
```

3. Audit Management initialisieren

```
DBMS_AUDIT_MGMT.INIT_CLEANUP(
  audit_trail_type          => DBMS_AUDIT_MGMT.AUDIT_TRAIL_ALL,
  default_cleanup_interval  => 24
);
```

4. Audit leeren

```
DBMS_AUDIT_MGMT.CLEAN_AUDIT_TRAIL(
  audit_trail_type => DBMS_AUDIT_MGMT.AUDIT_TRAIL_AUD_STD,
  use_last_arch_timestamp => TRUE
);
```

- Eigenen Tablespace definieren

```
DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_LOCATION(
  audit_trail_type => DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED,
  audit_trail_location_value => 'AUDSYS'
);
```

# Erstellen und Umsetzen von Audit Konzepten

## Vorbereitung

- Parameter des Unified Auditings

```
SQL> SELECT parameter_name, parameter_value, audit_trail
  1   FROM dba_audit_mgmt_config_params
  2*  WHERE audit_trail='UNIFIED AUDIT TRAIL';

PARAMETER_NAME                 PARAMETER_VALUE                AUDIT_TRAIL
------------------------------ ------------------------------ ----------------------------
AUDIT FILE MAX SIZE            10000                          UNIFIED AUDIT TRAIL
AUDIT FILE MAX AGE             5                              UNIFIED AUDIT TRAIL
DB AUDIT TABLESPACE            AUDSYS                         UNIFIED AUDIT TRAIL
AUDIT WRITE MODE               IMMEDIATE WRITE MODE           UNIFIED AUDIT TRAIL
```

- Audit Write Mode
  - Deprecated in 12.2

# Erstellen und Umsetzen von Audit Konzepten

## Vorbereitung

- Für 12.1 Datenbanken
  - Die Speicherung erfolgt intern in LOBs → schlechte Query Performance beim Auswerten
    - Performance Issues While Monitoring the Unified Audit Trail of an Oracle12c Database (Doc ID 2063340.1)
  - Überführen in eine relationale Speicherung (default ab 12.2)
    - Patch 25985768 oder Upgrade auf 12.2+
    - How To Transfer Unified Audit Records To An Internal Relational Table (Doc ID 2212196.1)

# Erstellen und Umsetzen von Audit Konzepten

## Umsetzung

- Regel 1: Alle Operationen, die SYS durchführt

```
create audit policy AP_SYS_OPERATIONS
actions
  all;

audit policy AP_SYS_OPERATIONS by SYS;
```

# Erstellen und Umsetzen von Audit Konzepten

## Umsetzung

- Regel 2: Änderungen am System, egal wer dies tut

```
create audit policy AP_SYSTEM_MGMT
actions
  create spfile,
  alter system,
  alter database;

audit policy AP_SYSTEM_MGMT;
```

# Erstellen und Umsetzen von Audit Konzepten

## Umsetzung

- Regel 3: Änderungen an Benutzern / Rollen, egal wer dies tut

```
create audit policy AP_USER_ROLE_MGMT
actions
  create user, alter user, drop user,
  create role, alter role, drop role, set role;

audit policy AP_USER_ROLE_MGMT;
```

# Erstellen und Umsetzen von Audit Konzepten

## Umsetzung

- Regel 4: Änderungen an Berechtigungen, egal wer dies tut

```
create audit policy AP_PRIVILEGE_MGMT
actions
  grant,
  revoke;

audit policy AP_PRIVILEGE_MGMT;
```

# Erstellen und Umsetzen von Audit Konzepten

## Umsetzung

- Regel 5: Änderungen an Auditing, egal wer dies tut

```
create audit policy AP_AUDIT_MGMT
actions
  audit, noaudit,
  create audit policy,
  alter audit policy,
  drop audit policy;

audit policy AP_AUDIT_MGMT;
```

# Erstellen und Umsetzen von Audit Konzepten

## Umsetzung

- Regel 6: An- und Abmeldungen an der Datenbank

```
create audit policy AP_LOGON_LOGOFF
actions
  logon,
  logoff;

audit policy AP_LOGON_LOGOFF;
```

# Erstellen und Umsetzen von Audit Konzepten

## Umsetzung

- Regel 7: Alle ANY-Privilegien

```
create audit policy AP_ANY_PRIVS
privileges
  create any table,
  drop any table,
  […]
;

audit policy AP_ANY_PRIVS;
```

# Erstellen und Umsetzen von Audit Konzepten

## Umsetzung

```
declare
  do_create boolean := true;
  do_sql varchar2(1000);
begin
  for privs in (select name from system_privilege_map where name like '% ANY %') loop
    if do_create then
     do_sql := 'create audit policy AP_ANY_PRIVS privileges ' || privs.name;
     do_create := false;
   else
     do_sql := 'alter audit policy AP_ANY_PRIVS add privileges ' || privs.name;
   end if;
   begin
     execute immediate do_sql;
   exception
     when others then
        dbms_output.put_line('skipping privilege "' || privs.name || '" due to: ' || SQLERRM);
   end;
  end loop;
end;
/
```

# Erstellen und Umsetzen von Audit Konzepten

## Umsetzung

- Regel 8: Änderungen an Wallets, egal wer dies tut

```
create audit policy AP_WALLET_MGMT
actions
  administer key management;

audit policy AP_WALLET_MGMT;
```

# Erstellen und Umsetzen von Audit Konzepten

## Umsetzung

- Applikationsspezifisches Auditing, Beispiel

```
create audit policy AP_ACCESS_TEST
actions
  select on test.test;

alter audit policy AP_ACCESS_TEST
add actions
  insert, update, delete on test.test;

alter audit policy AP_ACCESS_TEST
condition
  'SYS_CONTEXT(''USERENV'', ''CLIENT_IDENTIFIER'') = ''jdbc-thin'''
  evaluate per session;


audit policy AP_ACCESS_TEST;
```

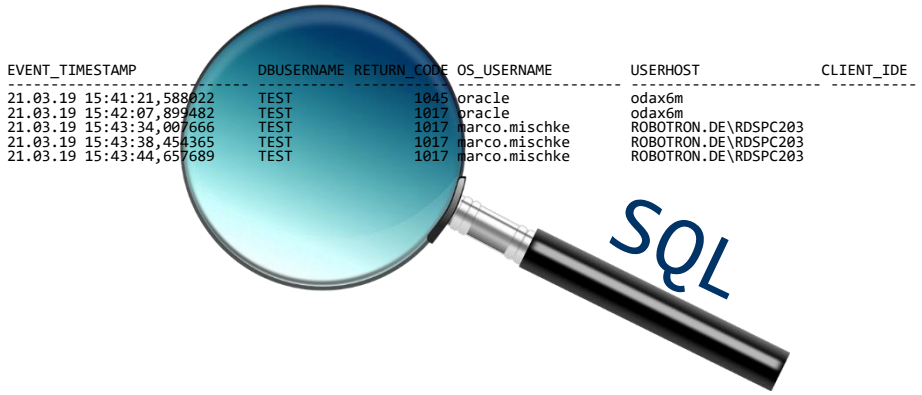
# Auswerten von Audit Daten

# Auswerten der Audit Daten

- Single Point of Truth → UNIFIED_AUDIT_TRAIL
- Erinnerung: Performance Probleme bei 12.1 → Patch erforderlich
  - Workaround: CREATE TABLE … AS SELECT …

- Persönliche SQL-Kenntnisse und Kreativität bestimmen die Grenzen

- Einige Beispiele….



# Auswerten der Audit Daten

- Wer verursacht fehlerhafte Login Versuche?

```
SQL> select EVENT_TIMESTAMP, DBUSERNAME, RETURN_CODE, OS_USERNAME, USERHOST, CLIENT_IDENTIFIER
2    from UNIFIED_AUDIT_TRAIL
3    where ACTION_NAME = 'LOGON'
4    and RETURN_CODE > 0;

EVENT_TIMESTAMP                DBUSERNAME RETURN_CODE OS_USERNAME          USERHOST                CLIENT_IDE
------------------------------ ---------- ----------- ------------------- ---------------------- ----------
21.03.19 15:41:21,588022       TEST              1045 oracle              odax6m
21.03.19 15:42:07,899482       TEST              1017 oracle              odax6m
21.03.19 15:43:34,007666       TEST              1017 marco.mischke       ROBOTRON.DE\RDSPC203
21.03.19 15:43:38,454365       TEST              1017 marco.mischke       ROBOTRON.DE\RDSPC203
21.03.19 15:43:44,657689       TEST              1017 marco.mischke       ROBOTRON.DE\RDSPC203
```

- Versucht da jemand, in die Datenbank einzubrechen?

# Auswerten der Audit Daten

- Wer hat da Daten manipuliert?

```
SQL> select event_timestamp, dbusername, return_code, sql_text
  2  from unified_audit_trail
  3  where object_schema='SCOTT'
  4  order by event_timestamp;

EVENT_TIMESTAMP           DBUSERNAME RETURN_CODE SQL_TEXT
------------------------- ---------- ----------- ------------------------------------------------------------
25.03.19 10:25:22,186080  SCOTT                0 select ename, sal from emp where mgr is null
25.03.19 10:25:44,679384  SCOTT                0 update emp set sal=2000 where mgr is null
25.03.19 10:25:53,434468  SCOTT                0 select ename from emp
25.03.19 10:26:11,696569  SCOTT                0 select ename, sal from emp where ename=user
25.03.19 10:26:30,110742  SCOTT                0 update emp set sal=6000 where ename=user
```

# Auswerten der Audit Daten

- Wer benutzt welche ANY-Privilegien und wofür?

```
SQL> select event_timestamp, dbusername, return_code, SYSTEM_PRIVILEGE_USED, sql_text
  2  from unified_audit_trail
  3  where UNIFIED_AUDIT_POLICIES like '%AP_ANY_PRIVS%'
  4  order by EVENT_TIMESTAMP;

EVENT_TIMESTAMP           DBUSERNAME RETURN_CODE SYSTEM_PRIVILEGE_USE SQL_TEXT
------------------------- ---------- ----------- -------------------- ----------------------------------
25.03.19 10:38:35,062842  TEST                0 SELECT ANY TABLE     select * from scott.emp
25.03.19 10:42:01,067653  TEST                0 CREATE ANY TRIGGER   create trigger scott.mod_emp
                                                                     before update on scott.emp
25.03.19 10:42:16,515381  TEST             4081 CREATE ANY TRIGGER   create trigger scott.mod_emp
                                                                     before update on scott.emp
25.03.19 10:42:42,817968  TEST                0 CREATE ANY TRIGGER   create or replace trigger
                                                                     scott.mod_emp
                                                                     before update on scott.emp
                                                                     for each row
```

# Housekeeping

# Housekeeping

- Dateien im Betriebssystem
  - Audit Informationen werden in $ORACLE_BASE/audit/$ORACLE_SID abgelegt, wenn die Datenbank nicht schreibbar ist (Startup, Read Only, …)
  - Audit Dateien können nachträglich geladen werden

```
DBMS_AUDIT_MGMT.LOAD_UNIFIED_AUDIT_FILES;
DBMS_AUDIT_MGMT.LOAD_UNIFIED_AUDIT_FILES(container => DBMS_AUDIT_MGMT.CONTAINER_ALL);
DBMS_AUDIT_MGMT.LOAD_UNIFIED_AUDIT_FILES(container => DBMS_AUDIT_MGMT.CONTAINER_CURRENT);
```

# Housekeeping

- Die Datenbank bringt Funktionen zum Löschen des (aller) Audit Trails mit
- Zwei Löschvarianten
  - Alles löschen
  - Alles älter als Zeitstempel löschen ← das will man meistens

- Idee: Audit Daten werden zuerst archiviert und danach gelöscht
  - Setzen des LAST_ARCHIVE_TIMESTAMP

# Housekeeping

- Löschen muss initialisiert werden

```
DBMS_AUDIT_MGMT.INIT_CLEANUP(
  audit_trail_type          => DBMS_AUDIT_MGMT.AUDIT_TRAIL_ALL,
  default_cleanup_interval  => 24
);
```

- Lösch-Job anlegen

```
DBMS_AUDIT_MGMT.CREATE_PURGE_JOB(
  audit_trail_type           => DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED,
  audit_trail_purge_interval => 24,
  audit_trail_purge_name     => 'CLEANUP_AUDIT_UNIFIED',
  use_last_arch_timestamp    => TRUE
);
```

# Housekeeping

- Löschen muss initialisiert werden

```
DBMS_AUDIT_MGMT.INIT_CLEANUP(
  audit_trail_type          => DBMS_AUDIT_MGMT.AUDIT_TRAIL_ALL,
  default_cleanup_interval  => 24
);
```

- Lösch-Job anlegen

```
DBMS_AUDIT_MGMT.CREATE_PURGE_JOB(
  audit_trail_type           => DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED,
  audit_trail_purge_interval => 24,
  audit_trail_purge_name     => 'CLEANUP_AUDIT_UNIFIED',
  use_last_arch_timestamp    => TRUE
);
```

# Housekeeping

- LAST_ARCHIVE_TIMESTAMP manuell oder automatisch setzen

```
begin
  dbms_scheduler.create_job(
    job_name   => 'CLEANUP_AUDIT_SET_TIMESTAMP',
    job_type   => 'PLSQL_BLOCK',
    job_action => 'begin
DBMS_AUDIT_MGMT.SET_LAST_ARCHIVE_TIMESTAMP(
 AUDIT_TRAIL_TYPE  => DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED,
 LAST_ARCHIVE_TIME => SYSTIMESTAMP - &DaysHistory.
);
end;',
    start_date      => trunc(systimestamp+1) + 1/24,
    repeat_interval => 'FREQ=HOURLY;INTERVAL=24',
     enabled         => true
  );
end;
```

Marco Mischke
Gruppenleiter Datenbank Projekte

Telefon: 0351 25859-2884
marco.mischke@robotron.de

www.robotron.de

@DBAMarco



MIT DATEN MEHR BEWEGEN.

robotron®