2015 DOAG Konferenz + Ausstellung

Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Geht Security in Oracle Database 12c eigentlich anders?

Heinz-Wilhelm Fabry
ORACLE Deutschland B.V. & Co. KG

ORACLE

Oracle Database 12*c* New Features Guide

2015 DOAG Konferenz + Ausstellung

Neue Security Features

- SHA-2
- Kontrolle von Program Units mit Caller's Rights
- SELECT ANY DICTIONARY
- Last Login Time Information
- Password Complexity Check
- Resource Role Default Privileges
- Unified Auditing
- Transparent Sensitive Data Protection
- VPD Fine-Grained Context-Sensitive Policies
- Restricted Service Registration für Oracle RAC
- Real Application Security
- Separation of Duties für DBAs

ORACLE

ORACLE | BU DB

4

Oracle Database 12*c* New Features Guide

2015 DOAG Konferenz + Ausstellung

Neue Security Features

- SHA-2
- Kontrolle von Program Units mit Caller's Rights
- SELECT ANY DICTIONARY
- Last Login Time Information
- Password Complexity Check
- Resource Role Default Privileges
- **Unified Auditing**
- Transparent Sensitive Data Protection
- VPD Fine-Grained Context-Sensitive Policies
- Restricted Service Registration für Oracle RAC
- Real Application Security
- **Separation of Duties für DBAs**

ORACLE

ORACLE | BU DB

5

Oracle Database 12*c* New Features Guide

2015 DOAG Konferenz + Ausstellung

Neue Security Features

- SHA-2
- Kontrolle von Program Units mit Caller's Rights
- SELECT ANY DICTIONARY
- Last Login Time Information
- Password Complexity Check
- Resource Role Default Privileges
- **Unified Auditing**
- Transparent Sensitive Data Protection
- VPD Fine-Grained Context-Sensitive Policies
- Restricted Service Registration für Oracle RAC
- Real Application Security
- **Separation of Duties für DBAs**

ORACLE

ORACLE | BU DB

Copyright © 2015, Oracle and/or its affiliates. All rights reserved.

6

Auditing - Ohne Kontrolle geht gar nichts (mehr)

Das A und O: Nachweisbarkeit

- BDSG (Anlage zu § 9 Satz 1)
  - Dabei sind insbesondere Maßnahmen zu treffen, die ... geeignet sind ... zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind ...
- PCI DSS (Requirement 10)
  - Track and monitor all access to network resources and cardholder data
- EUROSOX (8. EU Richtlinie)
  - Einrichtung und Prüfung interner Kontrollsysteme
- ...

ORACLE | BU DB

7

Auditing - Methoden

- Anwendungen führen ihre eigenen Protokolle
- Analyse von Redo Log-Dateien mit LogMiner
- Trigger
- Auditing durch die Datenbank

ORACLE | BU DB

8

Auditing durch die Datenbank

- Default Auditing
  - -> Betriebssystem
- Standard Auditing (Systemprivilegien, Befehle, Objekte)
  - -> SYS.AUD$ oder Betriebssystem in proprietärem Format oder XML
- Fine Grained Auditing ((FGA) - Auditieren abhängig von Bedingungen)
  - -> SYS.FGA_LOG$ oder Betriebssystem in proprietärem Format oder XML
- SYS Auditing
  - -> Betriebssystem
- Database Vault Auditing
  - -> DVSYS.AUDIT_TRAIL$

Complexity is the worst enemy of security.

Bruce Schneier
Secrets & Lies, Indianapolis 2004, S. 354

2015 DOAG Konferenz + Ausstellung

unified auditing

ORACLE

ORACLE | BU DB

2015 DOAG Konferenz + Ausstellung

Auditing Einrichten

Aktiviert oder nicht aktiviert?

- Verfügbar in allen Editionen
  - Kein Feature, das nur in der Enterprise Edition verfügbar ist
  - Es handelt sich nicht um eine Option

```
SELECT value FROM v$option
WHERE parameter = 'Unified Auditing'
```

- FALSE = *unified auditing* ist NICHT DAS STANDARDAUDITINGVERFAHREN
  - *mixed mode auditing* = altes und neues Auditing sind beide aktiviert
  - Umfang des *unified auditing* entspricht etwa dem Default von 11*g* AUDIT_TRAIL=DB
  - Nach einem Upgrade gelten die alten Audit Einstellungen nach wie vor

ORACLE

ORACLE | BU DB

Auditing Einrichten

Aktivieren des *unified auditing* als EINZIGES Verfahren

- Aktivieren ist über den Enterprise Manager oder Kommandozeile möglich
  - Datenbank und Listener stoppen

```
cd $ORACLE_HOME/rdbms/lib
make -f ins_rdbms.mk uniaud_on ioracle
                                    -- mit uniaud_off zurück zu mixed mode
```

  - Initialisierungsparameter wie AUDIT_TRAIL oder AUDIT_TRAIL_DEST werden ignoriert
  - Bereits gespeicherte Audit Daten werden NICHT gelöscht
  - 'Alte' Befehle werden NICHT mit Fehlermeldung zurückgewiesen, zum Beispiel

```
AUDIT ALL ON scott.emp
```

ORACLE | BU DB

Auditing Konfigurieren

Voraussetzungen

- Systemprivileg AUDIT SYSTEM
  - Darf das Auditing konfigurieren, aktivieren, de-aktivieren, aber nicht auswerten
- Rolle AUDIT_ADMIN
  - Darf das Auditing konfigurieren und auswerten
- Rolle AUDIT_VIEWER
  - Darf nur den *audit trail* auswerten, typischerweise Auditoren
- **Eigentümer eines Objekts kann nicht mehr**
  - **Das Auditing für diese Objekte selbst festlegen**
  - **Die über seine Objekte gesammelten Audit Daten auswerten**

ORACLE | BU DB

Auditing Konfigurieren

Befehl CREATE POLICY

- Vergleichbar mit dem Einrichten des FGA nutzt das *unified auditing* Policies
  - Standardmässig ist eine Policy mit dem Namen ORA_SECURECONFIG eingeschaltet
    - Entspricht etwa dem Default von 11*g* AUDIT_TRAIL=DB

```
CREATE AUDIT POLICY doag2015
PRIVILEGES    SELECT ANY TABLE
ACTIONS       CREATE USER, ALTER USER, SELECT ON SCOTT.EMP
ROLES         RESOURCE
WHEN 'SYS_CONTEXT("USERENV", "MODULE") <> ("HR")'
EVALUATE      PER STATEMENT
```


Auditing Konfigurieren

Hinweise zum CREATE POLICY

- Eigentümer der Policies ist SYS
- Es können beliebig viele Policies angelegt werden
  - Weniger ist mehr
    - Jede zu aktivierende Policy erhöht den Overhead beim Einloggen
    - Daten zu den Policies erhöhen den Speicherplatzbedarf in den UGAs
    - Performance wird durch die Auswertung vieler, konkurrierender Policies beeinträchtigt
- *unified auditing* erlaubt nicht das Auditieren auf der Grundlage von Spaltenwerten
  - FGA steht nach wie vor (nur) in der Enterprise Edition zur Verfügung

Auditing Konfigurieren

Komponenten auditieren

- Komponenten sind
  - Data Pump
  - Database Vault
  - Data Mining
  - Label Security
  - Real Application Security (RAS)
  - SQL Loader direct loads
- RMAN steuert sein Auditing über seinen Aufruf

```
CREATE AUDIT POLICY doag2015dp
   ACTIONS  COMPONENT =
                        DATAPUMP ALL

-- IMPORT oder EXPORT zur separaten Steuerung
```


Auditing Konfigurieren

Policies ändern oder löschen

```
ALTER AUDIT POLICY   doag2015
ADD              PRIVILEGES drop any table
DROP             ROLE resource
CONDITION    'SYS_CONTEXT(''USERENV'', ''IP_ADDRESS'') <>
                                                  (''111.112.113.114'')'
EVALUATE         PER STATEMENT
/
DROP AUDIT POLICY doag2015
/
```

Auditing aktivieren

Befehl AUDIT

- Anlegen der Policy allein genügt NICHT

```
AUDIT POLICY doag2015
EXCEPT SYS
```

- Gilt für alle Benutzer
  - Kein separates Auditing für SYS
  - Klausel EXCEPT erlaubt Ausschlüsse!
- Kann auch mit BY auf bestimmte Benutzer eingeschränkt werden
- Klausel WHENEVER (NOT) SUCCESSFUL steht ebenfalls zur Verfügung

Policy deaktivieren

Befehl NOAUDIT

```
NOAUDIT POLICY doag2015
BY scott
```

  - Klausel EXCEPT nicht erlaubt

Im Lieferumfang enthaltene Policies

- ORA_SECURECONFIG (enabled)
  - Entspricht den aus Oracle Database 11*g* bekannten Defaults
- ORA_ACCOUNT_MGMT (disabled)
  - CREATE / ALTER / DROP USER
  - CREATE / ALTER / DROP / SET ROLE
  - GRANT, REVOKE
- ORA_DATABASE_PARAMETER (disabled)
  - ALTER DATABASE
  - ALTER SYSTEM
  - CREATE SPFILE

Mandatory Auditing

- Befehle im Rahmen des Startup oder Befehle, die abgesetzt werden, wenn die Datenbank nicht zum Schreiben zur Verfügung steht, werden auf der Betriebssystemebene erfasst
  - $ORACLE_BASE/audit/$ORACLE_SID
  - Die Audit Daten können später in die Datenbank geladen werden
    - DBMS_AUDIT_MGMT.LOAD_UNIFIED_AUDIT_FILES
      - Nur SYS und AUDIT_ADMIN haben Ausführungsberechtigung für das Package DBMS_AUDIT_MGMT
      - Jede Ausführung des Package wird auditiert
    - Laden großer Datenmengen beeinflusst eventuell die DB Performance
- Alle Befehle, die das Auditing Verhalten beeinflussen
- Alle Befehle, die die Konfiguration von Database Vault beeinflussen

Monitoring

- AUDIT_UNIFIED_POLICIES
  - policy_name, audit_condition, condition_eval_opt, audit_option, audit_option_type, object_schema, object_name, object_type, common
- AUDIT_UNIFIED_ENABLED_POLICIES
  - user_name, policy_name, enabled_opt, success, failure
- AUDIT_UNIFIED_POLICY_COMMENTS
  - policy_name, comments

 23

Audit Daten auswerten

- Für die Auswertung benötigte Privilegien
  - AUDIT_ADMIN oder AUDIT_VIEWER
- UNIFIED_AUDIT_TRAIL
  - AUDIT_TYPE, DBUSERNAME, EVENT_TIMESTAMP, OBJECT_NAME, SQL_TEXT, SYSTEM_PRIVILEGE_USED, UNIFIED_AUDIT_POLICIES, ...
- CDB_UNIFIED_AUDIT_TRAIL
  - In einer PDB Äquivalent zum View DBA_*
  - Im Root einer CDB Informationen zu allen Audit Einträgen einschliesslich der Information in welcher PDB der Eintrag ausgelöst wurde
    - Klausel CONTAINER_DATA des Befehls ALTER USER legt fest, aus welchen PDBs Audit Daten angezeigt werden

 24

Konfiguration für Fortgeschrittene

Persistenz

- Audit Daten werden in eine Read Only Tabelle im Tablespace SYSAUX geschrieben
  - Eigentümer der Tabelle ist der Benutzer AUDSYS
  - Tabelle kann mit dem Package DBMS_AUDIT_MGMT in ein anderes Tablespace verschoben werden
  - Tabelle kann NICHT mit SQL Befehlen manipuliert werden, sondern aussschliesslich mit dem Package DBMS_AUDIT_MGMT

Konfiguration für Fortgeschrittene

Schreiben der Audit Daten

- Audit Daten werden über eine Queue in der SGA in die Datenbank geschrieben
  - Grösse der Queue wird bestimmt durch den Initialisierungsparameter UNIFIED_AUDIT_SGA_QUEUE_SIZE
    - 1 (Default) - 30 MB
  - Durch asynchrones Schreiben deutliche bessere Performance
  - Schreibintervall mit dem Package DBMS_AUDIT_MGMT auf synchron umzustellen
  - Schreiben der Queue kann mit dem Package DBMS_AUDIT_MGMT auch manuell veranlasst werden

Konfiguration für Fortgeschrittene

Audit Trail sichern und pflegen

- Gemäss geltender Regeln den *audit trail* sichern
  - Beispiel

```
INSERT INTO auditsicherung
SELECT * FROM UNIFIED_AUDIT_TRAIL;
```

- Gesicherte Einträge des *audit trail* mit dem Package DBMS_AUDIT_MGMT entweder über einen Job oder bei Bedarf in der Datenbank löschen
  - Der *audit trail* enthält immer mindestens als letzten Eintrag die Information zum letzten Löschvorgang

Konfiguration für Fortgeschrittene

Beispiel zum Löschen des *audit trail* nach dem Sichern

```
BEGIN DBMS_AUDIT_MGMT.CREATE_PURGE_JOB(
  AUDIT_TRAIL_TYPE                    =>
                        DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED,
  AUDIT_TRAIL_PURGE_INTERVAL    => 24,
  AUDIT_TRAIL_PURGE_NAME          => 'Audit_Cleanup',
  USE_LAST_ARCH_TIMESTAMP       => TRUE,
  CONTAINE                            =>
                         DBMS_AUDIT_MGMT.CONTAINER_CURRENT);
END;
```

Konfiguration für Fortgeschrittene

Views für das Arbeiten mit DBMS_AUDIT_MGMT

- DBA_AUDIT_MGMT_CLEAN_EVENTS
- DBA_AUDIT_MGMT_CLEANUP_JOBS
- DBA_AUDIT_MGMT_CONFIG_PARAMS
- DBA_AUDIT_MGMT_LAST_ARCH_TS

Detection is much more important than prevention.

Bruce Schneier
Secrets & Lies, Indianapolis 2004, S. 374

Oracle Database 12*c* New Features Guide

Neue Security Features

- SHA-2
- Kontrolle von Program Units mit Caller's Rights
- SELECT ANY DICTIONARY
- Last Login Time Information
- Password Complexity Check
- Resource Role Default Privileges
- **Unified Auditing**
- Transparent Sensitive Data Protection
- VPD Fine-Grained Context-Sensitive Policies
- Restricted Service Registration für Oracle RAC
- Real Application Security
- **Separation of Duties für DBAs**

Funktionen trennen, Aufgaben verteilen

Privilegien für Tätigkeiten, die nicht nur das laufende System betreffen

	Startup/ Shutdown	Alter DB OPEN, MOUNT, BACKUP	Alter DB Recover	Alter DB Archivelog	Alter DB Change Character Set	Create/ Drop DB	Create SPFILE	Restricted Session	Schema / Grund-privilegien
SYSDBA	☺	☺	☺	☺	☺	☺	☺	☺	SYS
SYSOPER	☺	☺	☺ vollst.	☺	☹	☹	☺	☺	PUBLIC

- Oft müssen mehr Rechte vergeben werden als notwendig
  - SYSDBA für Backups mit RMAN

Funktionen trennen, Aufgaben verteilen

least privilege

	Startup/ Shutdown	Alter DB OPEN, MOUNT, BACKUP	Alter DB Recover	Alter DB Archivelog	Alter DB Change Character Set	Create/ Drop DB	Create SPFILE	Restricted Session	Schema / Grund-privilegien
SYSDBA	☺	☺	☺	☺	☺	☺	☺	☺	SYS
SYSOPER	☺	☺	☺ vollst.	☺	☹	☹	☺	☺	PUBLIC
SYSBACKUP	☺	☺	☺	☺	☺	☺ Create	☺	☺	SYSBACKUP
SYSDG	☺	☺	☺	☺	☺	☹	☺	☺	SYSDG
SYSKM	☹	☹	☹	☹	☹	☹	☹	☺	SYSKM

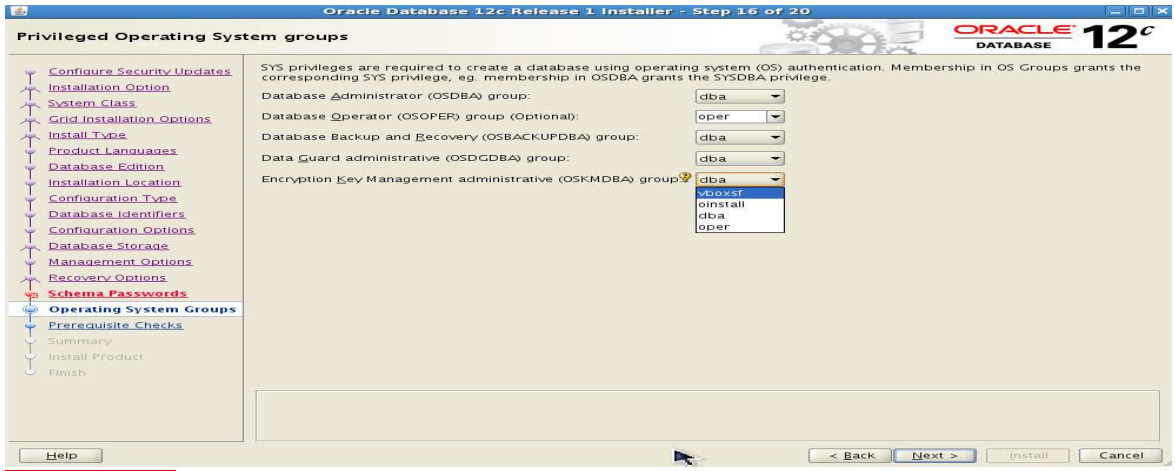
Beispiel SYSKM

Key Management Operationen (Wallet / Keystore – ASO)

- ADMINISTER KEY MANAGEMENT
- CREATE SESSION
  - Auch zum Anmelden bei einer nicht geöffneten Datenbank
- SELECT (bei geöffneter Datenbank)
  - SYS.V$ENCRYPTED_TABLESPACES
  - SYS.V$ENCRYPTION_WALLET
  - SYS.V$WALLET
  - SYS.V$ENCRYPTION_KEYS
  - SYS.V$CLIENT_SECRETS
  - SYS.DBA_ENCRYPTION_KEY_USAGE

SYSKM

Für alle Operationen, bei denen die Datenbank geschlossen ist



Informationen in deutscher Sprache

- Communities
  - DBA Community
  - APEX Community
  - Security Community
- Mobile App der BU DB
  - http://tinyurl.com/oracl
- DOAG
  - Competence Center Security

2015 DOAG Konferenz + Ausstellung

Integrated Cloud

Applications & Platform Services

ORACLE

ORACLE | BU DB

ORACLE