Menschen. Innovationen. Lösungen.

Database Vault und TDE
Ein Erlebnisbericht zur Einrichtung.

OPITZ CONSULTING

Database Vault und TDE

Ein Erlebnisbericht zur Einrichtung

Stefan Seck

Senior Consultant

OPITZ CONSULTING GmbH

DOAG Datenbank Konferenz 2015, Düsseldorf, 16.06.2015

Agenda

1. Motivation
2. Database Vault
3. Transparent Data Encryption
4. Demo
5. Zusammenfassung

1 Motivation

Motivation

- **Stand vor Projektstart**
  - Informationen wurden dezentral per Fax oder telefonisch gesammelt.
  - Wenige Personen haben Daten in Excel eingegeben.
  - Geschäftsführung hatte Zugriff auf das Excelsheet.
- **Wunsch**
  - Entlastung der MA
  - Moderne und automatisierte Anlage der Daten
  - Bessere Auswertbarkeit der Daten.
  - Trotzdem soll nur ein sehr begrenzter Zugriff erlaubt sein.
- **Vorgehen**
  - Klärung Sicherheitsanforderungen
  - Analyse der Schemata und Zugriffe
  - Aufbau Database Vault und TDE

Security im DB Umfeld

- **Präventiv**
  - Verschlüsselung
  - Data Masking
  - Kontrolle über „SuperUser“
  - …
- **Aktiv**
  - Auditierung der Zugriffe
  - Database Firewall
  - …
- **Administrativ / Organisatorisch**
  - Analyse der benötigten Privilegien
  - Aufteilen der benötigten Rollen
  - …

2 Database Vault

Warum Database Vault?

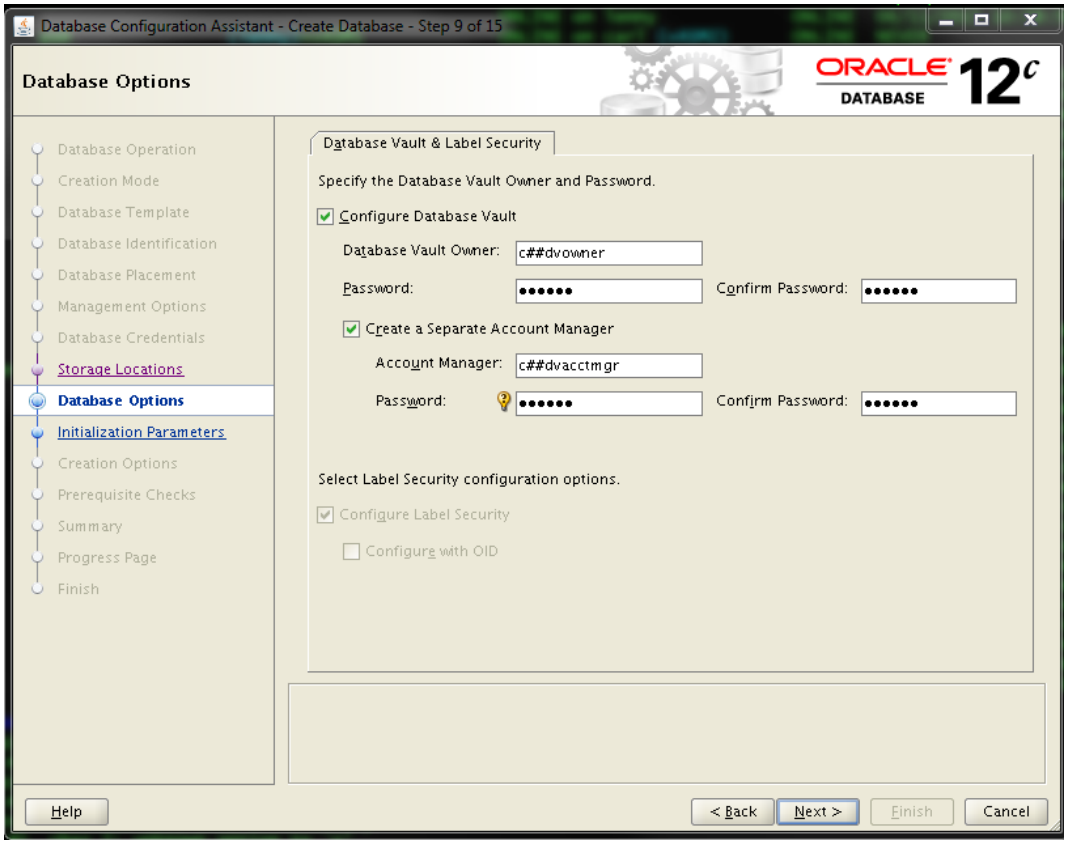
- **Zugriff auf Applikationsdaten werden geschützt**
- **Konsolidierung von Datenbanken / Schemata erfordern genauere Zugriffsrechte und Prüfungen**
- **“Interne” Bedrohungen müssen ernstgenommen werden**
- **Gesetzliche (SOX, Basel, PCI DSS, etc.) und interne Vorgaben**

Database Vault - Key Feature

- **„Separation of Duty“**
  - Rollentrennung DBA – Applikation
  - DBA kann keine Poweruser anlegen
  - Schützt DB Objekte vor Zugriff (Realms)
  - Verhindert die Ausführung von SQL Kommandos (Command Rules)

Installation

- **Mit 12c ist Database Vault schon im Kernel mitgeliefert**
- **Es reicht ein „einfaches“ Einschalten**



Einschalten Database Vault

- Als sysdba

```
BEGIN
 DVSYS.CONFIGURE_DV (
   dvowner_uname          => 'c##dvowner',
   dvacctmgr_uname        => 'c##dvacctmgr');
 END;
/
```

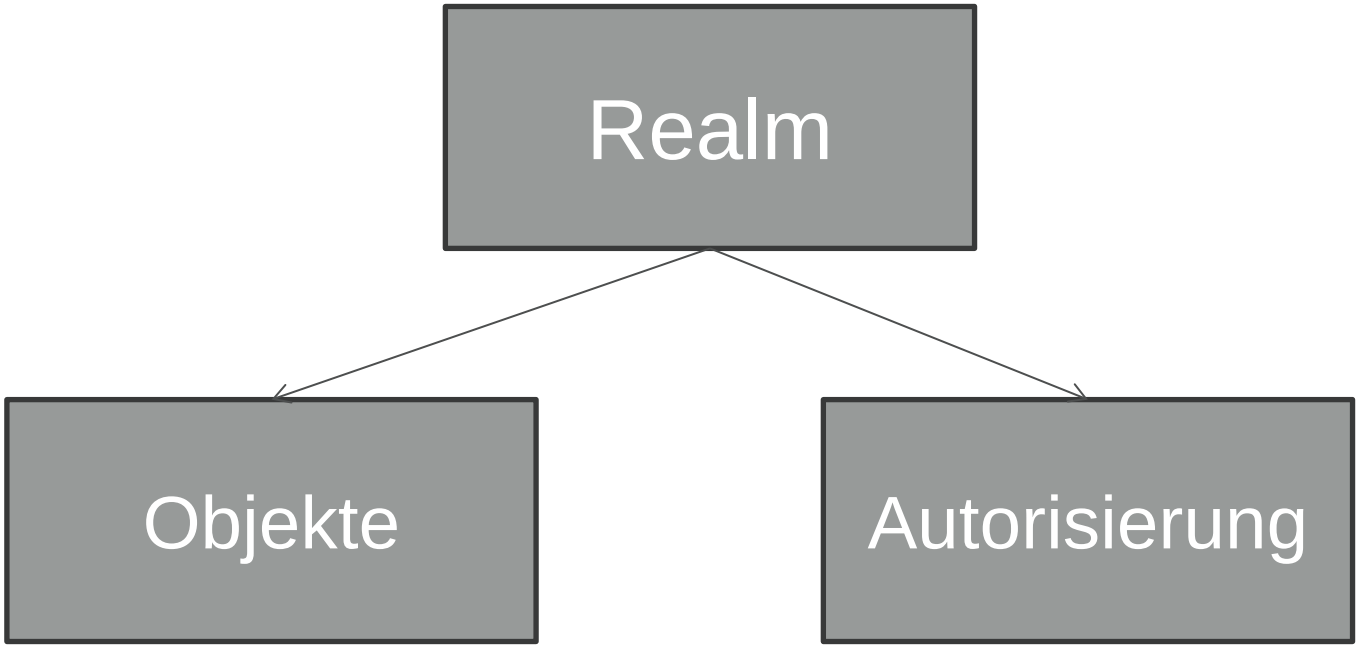
- Als Security Admin

```
EXEC DBMS_MACADM.ENABLE_DV;
```

- Restart der DB, bzw erneutes Öffnen der PDB

Realm anlegen

- **Ein Realm bildet eine Schutzzone um sensible Daten**



Administrative Aufgaben

- **Data Pump**
  - Exec dvsys.dbms_macadm.authorize_datapump_user
- **Jobs**
  - Exec dvsys.dbms_macadm.authorize_scheduler_user
- **DB Patching**
  - Rolle DV_PATCH_ADMIN muss zugewiesen sein
- **Explain Plan**
  - DBA braucht Schreibrechte an PLAN_TABLE

3

Transparent Data Encryption

TDE- Key Feature

- **Eingeführt mit Oracle 10g R2**
- **Es gibt einen Keystore für PDBs**
  - Zuerst in der CDBRoot öffnen
  - Dann in allen gewünschten PDBs
- **Verschlüsselt die Daten im SQL-Layer**
- **Einschränkungen bei Spaltenverschlüsselung:**
  - Keine MView Logs
  - Keine Lobs
  - Kein Streams oder CDC
  - Keine Transportable Tablespaces

TDE Keystore anlegen

- **In Oracle 11g**

```
ALTER SYSTEM SET ENCRYPTION KEY IDENTIFIED BY
“mypassword”
alter system set wallet open IDENTIFIED BY
“mypassword”;
```

- **Seit Oracle 12c**
  - Keystore anlegen

```
ADMINISTER KEY MANAGEMENT CREATE KEYSTORE
'/u01/app/oracle/admin/SSE121D1/enc_key/' IDENTIFIED BY
myPassword;
```

  - Keystore anlegen und öffnen

```
ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED
BY myPassword CONTAINER=ALL;
```

  - Keystore initialisieren

```
ADMINISTER KEY MANAGEMENT SET KEY IDENTIFIED BY
myPassword WITH BACKUP CONTAINER=ALL;
```

Verschlüssung

```
create tablespace ts_hr_enc
      DATAFILE '+DATA' size 10M autoextend on
      next 1M maxsize 50M
      ENCRYPTION USING 'AES256'
      DEFAULT STORAGE(ENCRYPT);

CREATE TABLE tde_test
      ( id NUMBER(10),
        data VARCHAR2(50) ENCRYPT );
```

- **Lobs**
  - Entweder in verschlüsselten Tablespaces
  - Oder in SecureFiles ablegen

Backups und Data Pump

- **RMAN nutzt TDE Wallet**

```
SET ENCRYPTION IDENTIFIED BY mypassword ON
FOR ALL TABLESPACES;
```

- **Data Pump**

```
expdp stefan_dba@pdv2 tables=hr_enc.employees
directory=dv_pump encryption=all
```

```
Vorsicht ohne encryption=XX:
ORA-39327: Oracle Database Vault data is being
stored unencrypted in dump file set.
```

4 Demo

5 Zusammenfassung

Zusammenfassung

- **Database Vault schottet Daten vor unerlaubtem Zugriff ab**
- **Rollenverteilung beachten und einhalten**
- **TDE verursacht Overhead durch ver- und entschlüsseln**
- **Bei Indizes aufpassen (Range Scan / Salt)**

- **MOS**
  - Master Note For Oracle Database Vault (Doc ID 1195205.1)
  - Master Note For Transparent Data Encryption (TDE) (Doc ID 1228046.1)

Fragen und Antworten

Kontakt

Stefan Seck
Senior Consultant

OPITZ CONSULTING Deutschland GmbH
Kirchstr. 6 | 51647 Gummersbach
Tel. +49 (2261) 60 01-0
stefan.seck@opitz-consulting.com

youtube.com/opitzconsulting

@OC_WIRE

slideshare.net/opitzconsulting

xing.com/net/opitzconsulting