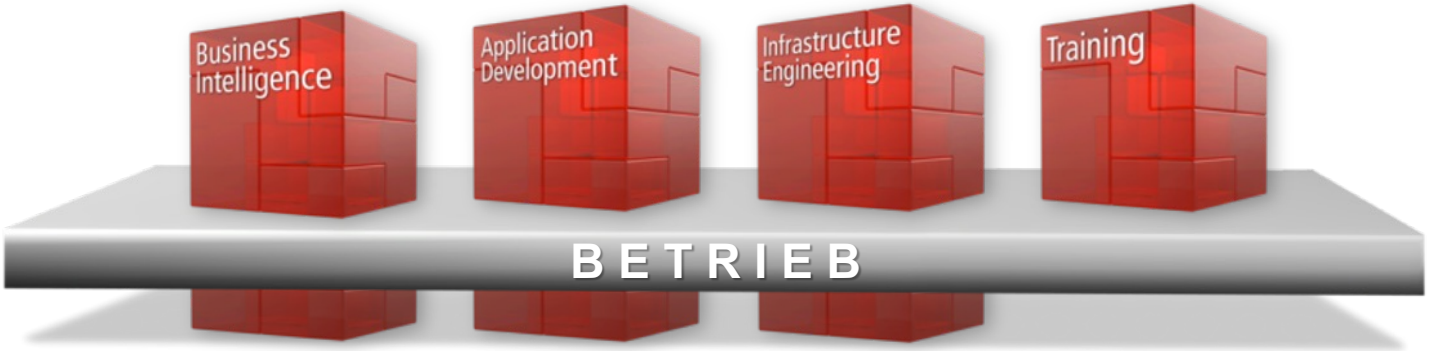
Oracle TSDP

Transparent Sensitiv Data Protection

Stefan Oehrli

Unser Unternehmen.

Trivadis ist führend bei der IT-Beratung, der Systemintegration, dem Solution Engineering und der Erbringung von IT-Services mit Fokussierung auf ORACLE - und Microsoft -Technologien in der Schweiz, Deutschland, Österreich und Dänemark. Trivadis erbringt ihre Leistungen aus den strategischen Geschäftsfeldern:



Trivadis Services übernimmt den korrespondierenden Betrieb Ihrer IT Systeme.

trivadis makes IT easier.

Mit über 600 IT- und Fachexperten bei Ihnen vor Ort.

- 14 Trivadis Niederlassungen mit über 600 Mitarbeitenden.
- Über 200 Service Level Agreements.
- Mehr als 4'000 Trainingsteilnehmer.
- Forschungs- und Entwicklungsbudget: CHF 5.0 Mio.
- Finanziell unabhängig und nachhaltig profitabel.
- Erfahrung aus mehr als 1'900 Projekten pro Jahr bei über 800 Kunden.

trivadis
makes IT easier.

Technik allein bringt Sie nicht weiter.

Man muss wissen, wie man sie richtig nutzt.

trivadis
makes IT easier.

Stefan Oehrli

Solution Manager BDS SEC / Trivadis Partner

- Seit 1997 im IT-Bereich tätig
- Seit 2008 bei der Trivadis AG
- Seit 2010 Disziplin Manager SEC INFR
- Seit 2014 Solution Manager BDS Security

IT Erfahrung

- DB Administration und DB Security Lösungen
- Administration komplexer, heterogenen Umgebungen
- Datenbank Teamleiter

Spezialgebiet

- DB Sicherheit und Betrieb
- Sicherheitskonzepte und deren Umsetzung
- Sicherheitsbewertungen
- Oracle Backup & Recovery
- Enterprise User Security und Oracle Unified Directory

Skills und Weiteres

- Backup & Recovery
- Oracle Advanced Security
- Oracle AVDF und DB Vault
- Oracle Directory Services
- Team / Projekt Management
- Referent O-SEC, O-BR,…

trivadis makes IT easier.

Agenda

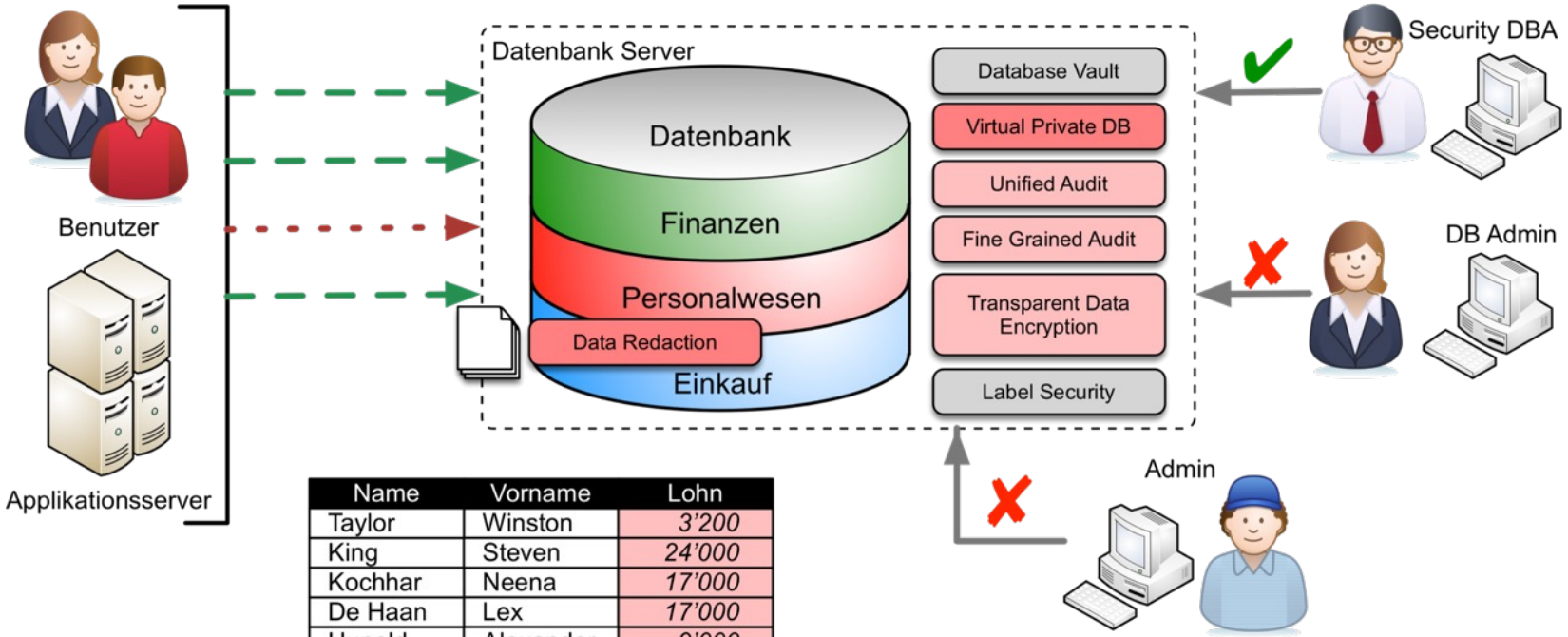
1. Einleitung
2. Separation of Duties (Rollentrennung)
3. Multitenant Umgebung
4. Step-by-Step
5. Data Dictionary Views
6. New Features Oracle 12.2
7. Herausforderungen und Use Cases
8. Fazit

trivadis makes IT easier.

Einleitung

trivadis
makes IT easier.

Herausforderung



Name	Vorname	Lohn
Taylor	Winston	*3'200*
King	Steven	*24'000*
Kochhar	Neena	*17'000*
De Haan	Lex	*17'000*
Hunold	Alexander	*9'000*
Ernst	Bruce	*6'000*
Austin	David	*4'800*

trivadis makes IT easier.

Herausforderung – Sensitive Informationen

- Verschiede Security Features nutzen Policies
  - Definition des Zugriff via **Virtual Private Database** Policy
  - Maskierung von Sensitiven Daten beim Zugriff mit **Data Redaction** Policy
  - Protokollierung des Zugriffs via **Audit Policy** oder **Fine Grained Audit** Policy
  - Verschlüsselung sensitiver Daten mit TDE Column
- Sensitive Informationen benötigen häufige mehrere Security Features z.B. VPD, Redaction und Audit
  - Redundante Policy Expression
  - Schwierig einheitliche und firmenweite Standards zu definieren

trivadis makes IT easier.

Transparent Sensitive Data Protection

- Transparent Sensitive Data Protection (TSDP) ist ein Weg um Spalten zu finden und zu klassifizieren, die sensitive (zu schützende) Informationen beinhalten.
- Festlegen von Sensitiven Datentypen innerhalb der Datenbank
- Klassifizierung der zu schützenden Daten
  - Z.B Sensitive Spalten mit Lohn, Kreditkarten Nummern etc.
- Schutz einer Klasse mit entsprechenden TSDP Policies
  - Schutz der Daten / Spalten mit VPD oder Data Redaction
  - Ab 12.2 Unified Auditing, FGA, TDE
  - Verwendung / Definition von uniformen Policies für alle klassifizierten Daten

trivadis makes IT easier.

Transparent Sensitive Data Protection

- Export TSDP Policies, Zuweisen der TSDP Policies in andere Datenbanken. (Firmenweiter Schutz)
- Integration im Oracle Entrperise Manager Cloud Control.
  - Application Data Modeling (ADM) Feature
  - Exportieren der zu schützenden Spalten. (XML)

trivadis makes IT easier.

TSDP Lizenzierung

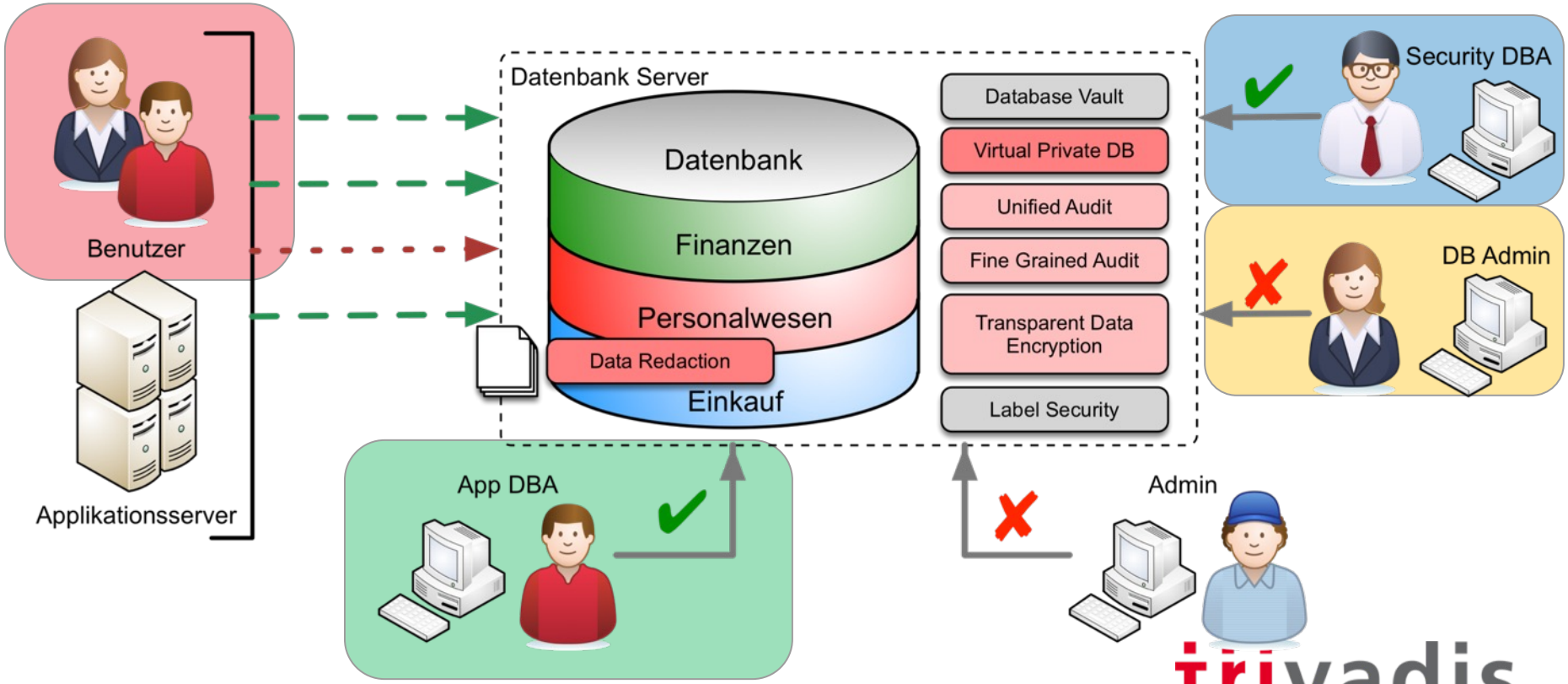
- Transparent Sensitive Data Protection ist ein Enterprise Feature
  - Oracle Enterprise Edition wird benötigt
- Weitere Lizenzen für die verwendeten Security Features z.B.
  - Oracle Advanced Security für TDE Column Encryption und Data Redaction
- Keine zusätzlichen Lizenzen für
  - Virtual Private Database
  - Unified Auditing
  - Fine Grained Audit

trivadis makes IT easier.

Separation of Duties (Rollentrennung)

trivadis makes IT easier.

Separation of Duties (Rollentrennung)



trivadis makes IT easier.

Separation of Duties (Rollentrennung)

- Zugriff auf folgende PL/SQL-Packages wird benötigt.
  - DBMS_TSDP_MANAGE
  - DBMS_TSDP_PROTECT
  - DBMS_REDACT
  - DBMS_RLS
- Weitere Rechte nach Bedarf z.B. für Unified Audit
- Application Database Administrator (APPADMIN)
  - DBMS_TSDP_MANAGE
- Security Database Administrator
  - DBMS_TSDP_PROTECT, DBMS_REDACT, DBMS_RLS (SECADMIN)

trivadis makes IT easier.

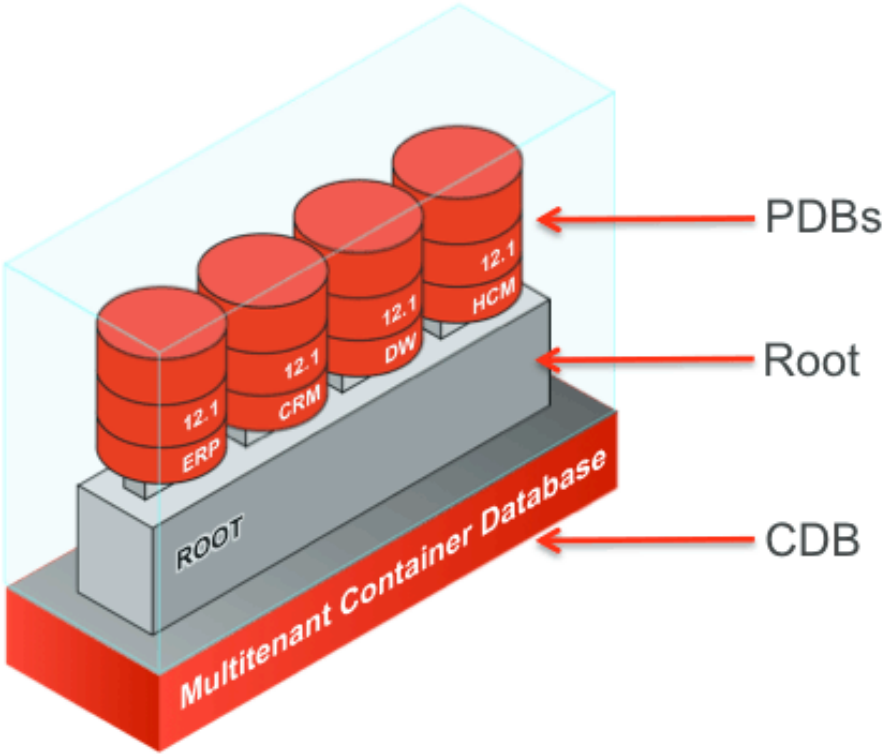
Multitenant Umgebung

trivadis
makes IT easier.

Multitenant Umgebung

- TSDP Policies können nur auf
  - die aktuelle PDB oder
  - die aktuelle Application PDB (siehe: New Feature 12.2, Application Containers)

  angewendet werden.
- Informationen findet man in
  - DBA_PDBS



trivadis makes IT easier.

Step-by-Step

trivadis
makes IT easier.

Step-by-Step

- Step 1: Erstellen Sensitive Type
  - mit Enterprise Manager Cloud Control Application Data Model
  - oder PL/SQL-Prozedur **dbms_tsdp_manage.add_sensitive_type**

```
SQL> BEGIN
       dbms_tsdp_manage.add_sensitive_type
         ( sensitive_type => 'gehalt_num_type',
           user_comment   => 'Type fuer Gehalt - Number Datatype ');
     END;
```

- Data Dictionary View
  - DBA_SENSITIVE_COLUMN_TYPES

trivadis makes IT easier.

Step-by-Step

- Step 2: Identifizieren der sensitiven Spalten
  - mit Enterprise Manager Cloud Control Application Data Model
  - oder PL/SQL-Prozedur **dbms_tsdp_manage.add_sensitive_column**

```
SQL> BEGIN
       dbms_tsdp_manage.add_sensitive_column
         ( schema_name    => 'SCOTT',
           table_name     => 'EMP',
           column_name    => 'SAL'
           sensitive_type => 'gehalt_num_type',
           user_comment   => 'Zuweisung SAL zu gehaltnum_type' );
     END;
```


trivadis makes IT easier.

Step-by-Step

- Step 3: Importieren der sensitiven Spalten, wenn mit Enterprise Manager Cloud Control Application Data Model gearbeitet wurde.

  Ansonsten kann der Schritt übersprungen werden.

```
SQL> BEGIN
       DBMS_TSDP_MANAGE.IMPORT_DISCOVERY_RESULT
         ( discovery_result => xml_adm_result,
           discovery_source => 'ADM_Demo');
     END;
```

- Data Dictionary View
  - DBA_TSDP_IMPORT_ERRORS

trivadis makes IT easier.

Step-by-Step

- Step 4: Erstellen der Transparent Sensitive Protection Policy
  - für Oracle Virtual Private Database Settings oder Data Redaction konfigurierbar.

```
SQL> DECLARE -- Data Redaction Settings
       redact_feature_options DBMS_TSDP_PROTECT.FEATURE_OPTIONS;
       policy_conditions      DBMS_TSDP_PROTECT.POLICY_CONDITIONS;
     BEGIN
       redact_feature_options ('expression') := 'SYS_CONTEXT(''USERENV'',
                                                ''SESSION_USER'') =''HR''';
       redact_feature_options ('function_type') := 'DBMS_REDACT.FULL';
       dbms_tsdp_protect.add_policy ('MASK_GEHALT', DBMS_TSDP_PROTECT.REDACT,
                                     redact_feature_options,
                                     policy_conditions);
     END;
```


trivadis makes IT easier.

Step-by-Step

- Step 5: Verbinden der Policy mit dem Sensitiven Type

```
SQL> BEGIN
       dbms_tsdp_protect.associate_policy
         (policy_name => 'MASK_GEHALT',
          sensitive_type => 'gehalt_num_type',
          associate => true);
     END;
```

- Data Dictionary View
  - DBA_TSDP_POLICY_TYPE

trivadis makes IT easier.

Step-by-Step

- Step 6: Einschalten der Transparent Sensitive Data Protection Policy

```
SQL> BEGIN
       -- Einschalten fuer alle Spalten des Types.
       dbms_tsdp_protect.enable_protection_type
         (sensitive_typ => 'gehalt_num_type');
     END;
```

- Weitere Möglichkeiten
  - Einschalten für eine bestimmte Spalte
  - Einschalten aller Policies für eine Datenbank.
    DBMS_TSDP_PROTECT.ENABLE_PROTECTION_SOURCE

trivadis makes IT easier.

Step-by-Step

- Step 7: Exportieren/Importieren der Policy von/in eine andere Datenbank
  - Oracle DataPump
- Anmerkungen

  Policies können ausgeschaltet und gelöscht werden.
  - `DBMS_TSDP_PROTECT.DISABLE_PROTECTION_TYPE`
  - `DBMS_TSDP_PROTECT.DISABLE_PROTECTION_COLUMN`
  - `DBMS_TSDP_MANAGE.DROP_SENSITIVE_COLUMN`
  - `DBMS_TSDP_MANAGE.DROP_SENSITIVE_TYPE`
  - `DBMS_TSDP_PROTECT.DROP_POLICY`

trivadis makes IT easier.

Step-by-Step

- Transparent Sensitive Protection für VPD

```
CREATE OR REPLACE FUNCTION vpd_function ( v_schema IN VARCHAR2, v_objname IN
VARCHAR2)
 RETURN VARCHAR2 AS
BEGIN
 RETURN 'SYS_CONTEXT(''USERENV'',''SESSION_USER'') = ''SCOTT''';
END vpd_function;
```

```
SQL> DECLARE
       vpd_feature_options DBMS_TSDP_PROTECT.FEATURE_OPTIONS;
       policy_conditions   DBMS_TSDP_PROTECT.POLICY_CONDITIONS;
     BEGIN
       vpd_feature_options ('policy_function') := 'vpd_function';
       vpd_feature_options ('sec_relevant_cols_opt') := 'DBMS_RLS.ALL_ROWS';
     …
     END;
```


trivadis makes IT easier.

Data Dictionary Views

trivadis
makes IT easier.

Data Dictionary Views

- Transparent Sensitive Data Protection
  - DBA_TSDP_POLICY_FEATURE
  - DBA_TSDP_POLICY_PROTECTION
  - DBA_TSDP_POLICY_TYPE
  - DBA_TSDP_POLICY_PARAMETER

```
SQL> SELECT * from dba_tsdp_policy_parameter;

POLICY_NAME                    PARAMETER             VALUE
------------------------------ --------------------  ---------------------------------------------
TSDP_POL_REDACT_PROJECT_VALUE  expression            SYS_CONTEXT('USERENV', 'SESSION_USER') ='HR'
TSDP_POL_REDACT_PROJECT_VALUE  function_type         DBMS_REDACT.FULL
TSDP_POL_VPD_PROJECT_VALUE     policy_function       vpd_function
TSDP_POL_VPD_PROJECT_VALUE     sec_relevant_cols_opt DBMS_RLS.ALL_ROWS
```


trivadis makes IT easier.

Data Dictionary Views

Data Redaction

```
SQL> SELECT object_owner, object_name, policy_name
 2   FROM   redaction_policies;

OBJECT_OWNER OBJECT_NAME POLICY_NAME
------------ ----------- ------------------------------------------------------
SCOTT        EMP         ORA$REDACT_72DcBB5OcsEATBIuPE5pOMHekV7Bpf9vAsdtQ2miqC
                         VuLAG9E24RMzzw9QdPmM8wVyuXzUlYTynHelxd1B6RiPEifOfqBQe
                         z0qA3jZ80EXch5bJmUniK:
SCOTT        PROJECTS    ORA$REDACT_A7kWSnBeyAkFd9aIAnJOZTiE3OlKBNaGEu7l1L8uHR
                         Nis6DvNuJPrZ3ovFAnRkYwNMk9QIgoi9Mletw87wXMW3XS77lM0GL
                         A1Uy0BGs6Q8mvAzKjdJto:
```


trivadis makes IT easier.

Data Dictionary Views

Data Redaction

```
SQL> SELECT object_owner, object_name, column_name,
 2  function_type, function_parameters
 3  FROM   redaction_columns;

OBJECT_OWNER OBJECT_NAME COLUMN_NAME     FUNCTION_TYPE  FUNCTION_PARAMETERS
------------ ----------- --------------- -------------- --------------------
SCOTT        PROJECTS    PROJECT_VALUE   FULL REDACTION
SCOTT        PROJECTS    BUDGET_INTERN   FULL REDACTION
```


trivadis makes IT easier.

Data Dictionary Views

- Virtual Private Database (VPD)

```
SQL> SELECT object_owner, object_name, policy_name, pf_owner, function
     FROM   dba_policies
     WHERE  object_owner = 'SCOTT';

OBJECT_OWNER OBJECT_NAME POLICY_NAME                        PF_OWNER. FUNCTION
------------ ----------- ------------------------------- --------- ---------
SCOTT        PROJECTS    ORA$VPD_SF8ROQKW7BRIS4UVYWGCUIQT SECADMIN  VPD_FUNCTION
                         QOTHYVPC6KICT0EKY3WKWS4CMLZNFXJN
                         XKWYRJSRGTUU1CLVVOPCLAJLMARRFVRH
                         YPIDT5N59UKAR2UGSRFXCRLKNEYG2SH8
```


trivadis makes IT easier.

New Features Oracle 12.2

trivadis
makes IT easier.

New Features Oracle 12.2

- Verwendung von Transitive Sensitive Data Protection mit
  - Unified Auditing
  - Fine Grained Auditing
  - TDE Column Encryption

trivadis makes IT easier.

New Features Oracle 12.2

- Steuerung über Parameter: security_feature

```
dbms_tsdp_protect.add_policy (policy_name => '<poliy_name>',
              security_feature => DBMS_TSDP_PROTECT.UNIFIED_AUDIT,...

dbms_tsdp_protect.add_policy (policy_name => '<poliy_name>',
              security_feature => DBMS_TSDP_PROTECT.FINE__GRAINED_AUDIT,...

dbms_tsdp_protect.add_policy (policy_name => '<poliy_name>',
              security_feature => DBMS_TSDP_PROTECT.COLUMN_ENCRYPTION,...
```


trivadis makes IT easier.

TSDP und Unified Auditing – Voraussetzungen

- AUDIT SYSTEM Systemprivileg wird benötigt.
- Erstellen einer Policy mit den notwendigen Audit Settings
- Verbinden der Policy mit dem Sensitiven Type
- Einschalten der Transparent Sensitive Data Protection Policy.
- Beim Zugriff auf die geschützte Tabelle wird ein Eintrag im UNIFIED_AUDIT_TRAIL geschrieben.

trivadis makes IT easier.

New Features Oracle 12.2

```
SQL> declare
       audit_feature_options DBMS_TSDP_PROTECT.FEATURE_OPTIONS;
       policy_conditions     DBMS_TSDP_PROTECT.POLICY_CONDITIONS;
     begin
       audit_feature_options ('ACTION_AUDIT_OPTIONS') := 'ALL';
       audit_feature_options ('AUDIT_CONDITION')      := '<CONDITION>';
       audit_feature_options ('EVALUATE_PER')         := 'STATEMENT';
        dbms_tsdp_protect.add_policy
         (policy_name            => 'AUDIT_SAL',
          security_feature       => DBMS_TSDP_PROTECT.UNIFIED_AUDIT,
          policy_enable_options  => audit_feature_options,
…
```


trivadis makes IT easier.

New Features Oracle 12.2

- Transitive Sensitive Data Protection und Unified Auditing

```
SQL> …
       dbms_tsdp_protect.add_policy
         (policy_name            => 'AUDIT_SAL',
          security_feature       => DBMS_TSDP_PROTECT.UNIFIED_AUDIT,
          policy_enable_options  => audit_feature_options,
          policy_apply_condition => policy_conditions);
       dbms_tsdp_protect.associate_policy
         (policy_name    => 'AUDIT_SAL',
          sensitive_type => 'PROTECT_SAL');
     END;
```


trivadis makes IT easier.

TSDP und Unified Auditing – Audit Policy

- Interner Ablauf
  - Beim Einschalten der Policy wird eine interne TSDP Policy erstellt. ORA$UNIFIED_AUDIT_<random-number>

```
SQL> SELECT policy_name FROM audit_unified_policies
  2  WHERE policy_name LIKE 'ORA$%';

POLICY_NAME
--------------------------------------------------------------------------
ORA$UNIFIED_AUDIT_OUMZV9BVOBCZO2GGHLRQD3EZFSO8JWFVCKKPYBX5SN95BFNBEBKDLLA
A1BOTC8NOWJ5N1EQODPS3HVMNAEU20TAPNG8YNKP1IJDUDZQQMWYWHG
```


trivadis makes IT easier.

TSDP und Unified Auditing – Audit Einträge

- Eintrag im UNIFIED_AUDIT_TRAIL

```
SQL> SELECT event_timestamp, dbusername, action_name, object_name,
sql_text FROM unified_audit_trail WHERE dbusername='SCOTT'

EVENT_TIMESTAMP   DBUSERNAME ACTION_NAME OBJECT_NAME  SQL_TEXT
----------------- ---------- ----------- ------------ ----------------------------
18.04.18 09:41:22 SCOTT      SELECT      PROJECTS     select * from SCOTT.PROJECTS
```


trivadis makes IT easier.

TSDP und Fine Grained Audit

- Erstellen einer Policy mit den notwendigen Audit Settings
- Verbinden der Policy mit dem Sensitiven Type
- Einschalten der Transparent Sensitive Data Protection Policy. Es wird automatisch eine Fine Grained Audit Policy erstellt.
- Interner Ablauf
  - Beim Einschalten der Policy wird eine interne TSDP Policy erstellt. ORA$FGA_<random-number>

trivadis makes IT easier.

TSDP und TDE Column Encryption

- Erstellen einer Policy mit den notwendigen Encryption Settings
- Verbinden der Policy mit dem Sensitiven Type
- Einschalten der Transparent Sensitive Data Protection Policy.
- Mehre Policies mit unterschiedlichem Verschlüsselungsalgorithmus sind möglich, wobei der stärkste «gewinnt»
- Interner Ablauf
  - Beim Einschalten der Policy wird eine interne TSDP Policy erstellt.
  - ORA$TDECE_<random-number>

trivadis makes IT easier.

Herausforderungen und Use Cases

trivadis
makes IT easier.

TSDP und Unified Auditing – Bugs

- Wenn Condition = 'SYS_CONTEXT("USERENV", "SESSION_USER") IN ("HR","SCOTT")‘

```
*** 2017-10-12T09:19:39.753072+01:00 (AXK01)
Error : 45618 - TSDP Policy Enforcement failed
KZDP OCI Error -ORA-00905: missing keyword
ORA-45618 -  Creation of Unified Audit Policy on table 'EMP' in schema 'SCOTT'
failed.
```

- Workaround für Condition

  SYS_CONTEXT(""USERENV"", ""SESSION_USER"") IN (""HR"",""SCOTT"")

- Bug 27326938 : TSDP: AUDIT_FEATURE_OPTIONS NEEDS EXTRA SINGLE QUOTES

trivadis makes IT easier.

TSDP Herausforderungen

- Fine Grained Audit

```
ERROR at line 11:
ORA-06550: line 11, column 77:
PLS-00302: component 'FINE_GRAINED_AUDIT' must be declared
ORA-06550: line 10, column 3:
PL/SQL: Statement ignored
```

- TDE Column Encryption

```
*** 2017-10-13T08:06:55.437002+01:00 (AXK01)
Error : 45618 - TSDP Policy Enforcement failed
KZDP OCI Error -ORA-00942: table or view does not exist
```


trivadis makes IT easier.

TSDP Herausforderungen

- Korrekte Konfiguration/Parameter für die verschiedenen Security Features
- Dokumentation und Beispiele primär für VPD und Data Redaction
- Zusätzlich Rechte werden benötigt z.B. um Unified Audit Policies anzulegen

trivadis makes IT easier.

Use Cases

- Kombinierter Einsatz von verschiedenen Security Features Audit, VPD und Redaction
- Sensitive Daten können gleich respektive einheitlich geschützt werden
- Definition von firmenweiten Policies z.B
  - Lohnspalten werden in allen Anwendungen / Datenbanken gleich geschützt
  - Erfüllen von Compliance (PCI) und Datenschutzrechtlichen Auflagen (GDPR)

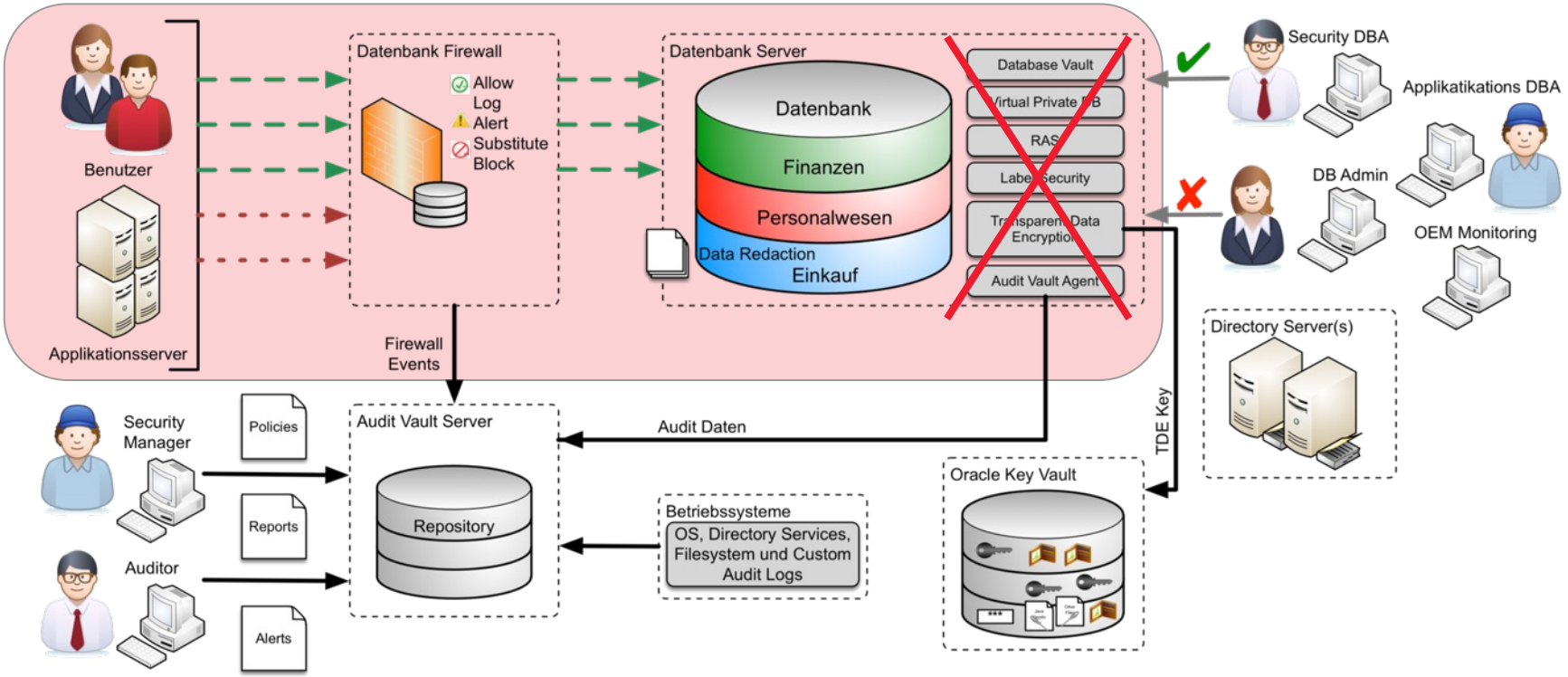
trivadis makes IT easier.

Alternativen

- Schutz der Daten von «ausserhalb» mit Oracle Audit Vault and Database Firewall oder Database Activity Monitoring
  - Unerlaubter Zugriff wird bereits vor der DB Blockiert
  - Keine Konfiguration / Anpassung der Applikation nötig
  - Funktioniert auch bei Standard Edition
  - Zentrales Audit und sammeln der Audit Events
- Zusätzliches Produkt benötigt Lizenzen, bindet Ressourcen und generiert Betriebsaufwand

trivadis makes IT easier.

Alternativen



trivadis makes IT easier.

Fazit

- TSDP ist eine sehr gute Möglichkeit sensitive Daten zu schützen
- Möglichkeit um firmenweiter Standards zu definieren und alle Sensitiven Daten gleich zu schützen.
- 12.2 Features laufen noch nicht ganz so „rund“

trivadis makes IT easier.

Weitere Informationen

- Oracle Dokumentation
  https://docs.oracle.com/en/database/oracle/oracle-database/18/dbseg/index.html
- Trivadis eXpert Team Security
  http://www.trivadis.com/de/security

trivadis makes IT easier.

Fragen und Antworten...

Stefan Oehrli
Solution Manager / Trivadis Partner

Tel.: +41 58 459 55 55
stefan.oehrli@trivadis.com

http://www.trivadis.com/security
http://www.oradba.ch
@stefanoehrli

trivadis makes IT easier.