Oracle 12c Real Application Security

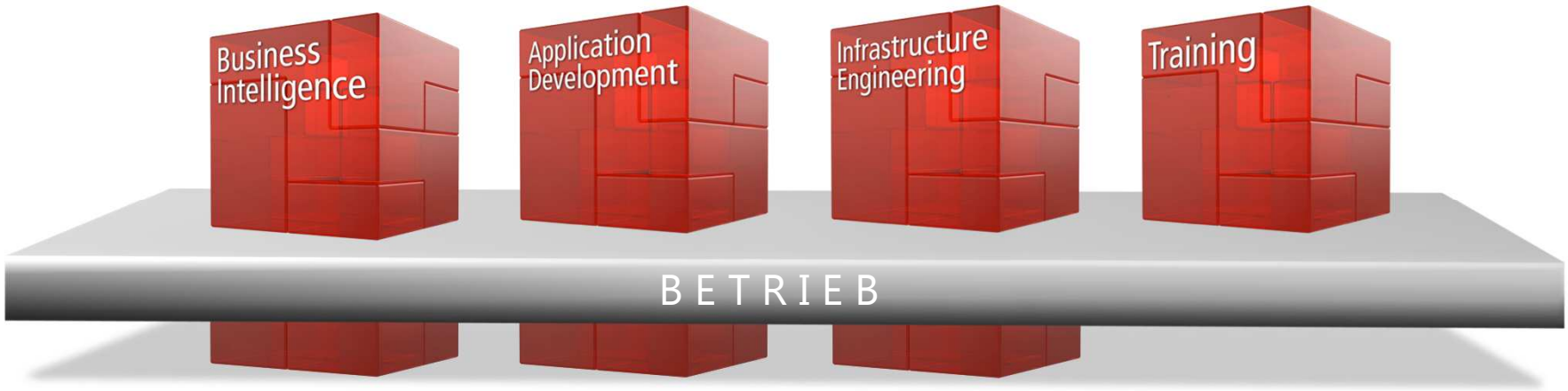
Basis Know-How

Axel Kraft
Senior Consultant

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 im D-A-CH-Raum.

Unsere Leistungen erbringen wir 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. / EUR 4.0 Mio.
- Finanziell unabhängig und nachhaltig profitabel.
- Erfahrung aus mehr als 1'900 Projekten pro Jahr bei über 800 Kunden.

trivadis makes IT easier.

Axel Kraft

Senior Consultant IMS

- Seit 1990 im IT-Bereich tätig
- Seit 2012 bei der Trivadis GmbH in Stuttgart

IT Erfahrung

- Consultant für Oracle Datenbank Administration und Oracle Datenbank Security Lösungen
- Administration von komplexen und heterogenen Oracle Datenbank Umgebungen

Spezialgebiet

- Oracle Datenbankbetrieb und Security
- Standardisierung Oracle Datenbankbetrieb
- Oracle Backup & Recovery

Skills

- Oracle Backup & Recovery
- Oracle Database Security
- Oracle Advanced Security Audit Vault und Database Firewall, Database Vault
- Oracle Database Administration

Hinweis

- Analysen, Meinungen und Darstellungen, die in dieser Präsentation geäußert werden, sind die des Autors.

  Sie wurden nicht mit Oracle abgestimmt.

Agenda

1. **Einleitung**
2. **Datensicherheitskonzepte**
3. **Oracle Database Real Application Security**
   - PL/SQL Packages/Functions - Data Dictionary Views
4. **Use Case**
5. **Konfiguration/Komponenten für den UseCase**
6. **Auditing**
7. **Fazit**
8. **Demo**

Einleitung

Einleitung

Oracle Database Security im klassischen Sinne …

- wurde für Client/Server Systeme konzipiert.
- hatte weniger Internet-Anwendungen mit vielen End-Usern abzusichern.
- verlegte Sicherheitseinstellungen der Datenbank in die Applikation.

Einleitung

Oracle Database 12c Real Application Security ist ein neues Konzept,…

- das Endbenutzer einer Anwendung in der Datenbank als Anwendungsbenutzer repräsentiert.
- welches Priviliegien die Anwendungsoperationen schützen, in der Datenbank definiert.
- den Context der Anwendungsbenutzer in der Datenbank als Session repräsentiert.
- das speziell für Multi-Tier Anwendungen (Internet-Anwendungen, WEB-Anwendungen) ausgelegt ist.

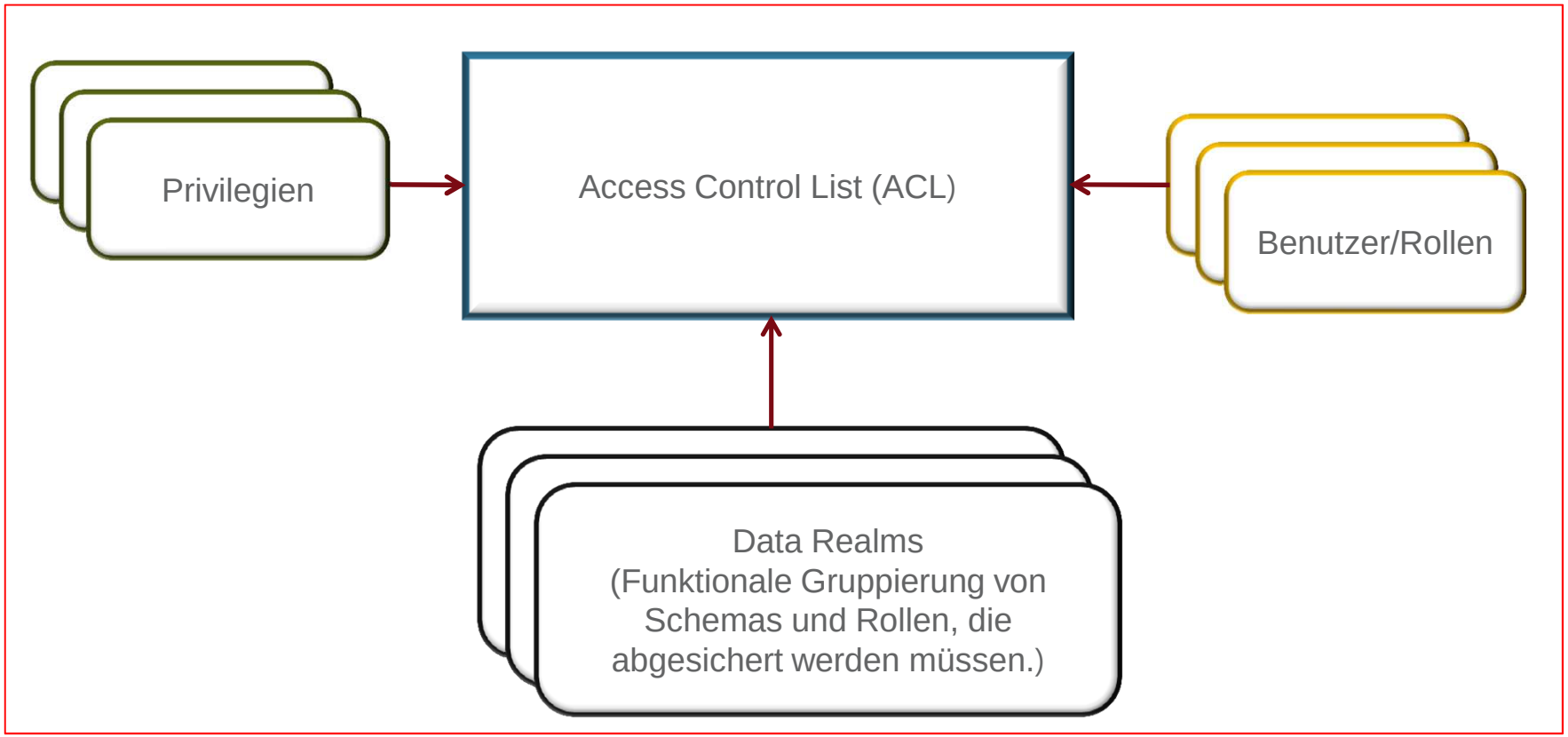
Einleitung

Oracle Database 12c Real Application Security ist …

- die nächste Generation der VPD. (Virtual Private Database)
- erfüllt die 3 Dimensionen der effektiven Sicherheit.
  - Welcher Applikationsbenutzer, welche Applikationen, welche Funktionen
  - können welche Operationen
  - auf welchen Daten ausführen.

Einleitung

Die drei Dimensionen der effektiven Datenbanksicherheit …



Einleitung

Nachteile der traditionellen Oracle Security um Applikationsbenutzer zu verwalten …

- Erweiterte Sicherheitsrichtlinien sind unabhängig von Applikations-Code.
- Durchsetzung von Sicherheitsichtlinien auf Datenbankebene mit unbekanntem Applikationsbenutzer.
- Durchsetzung von weniger Rechten.

Einleitung

Vorteile Oracle Database Real Application Security

- Three-tier und Two-tier Anwendungen können den Zugriff auf die Datenbank deklarativ bereitstellen und steuern.
- Die Datenbank kann ein einheitliches Sicherheitsmodell über alle Schichten zur Verfügung stellen.
- Die Datenbank speichert die Applikations-Sicherheitsinformationen. (Reduzierung des Netzwerk-Traffics)
- Oracle 12c Real Application Security ist in der Oracle Enterprise Edition enthalten. Also ist keine zusätzliche Lizens nötig. ☺

Datensicherheitskonzepte

Datensicherheitskonzepte

- Unterschied Datenbankbenutzer - Applikationsbenutzer
  - Datenbankbenutzer hat Schema und Password
  - Applikationsbenutzer hat keine eigenen Datenbankschemas, kann Sessions anlegen in der Middle-Tier. Werden durch die Applikation definiert.
- Unterschied Datenbankrolle – Applikationsrolle
  - Eine Datenbankrolle besteht aus Datenbankprivilegien
  - Applikationsrolle besteht aus applikationsdefinierten Privilegien sowie deklarativen Access Control Lists (ACL)
- Datenbankprivilegien können nicht direkt an Applikationsbenutzer, -rollen vergeben werden.
- Datenbankprivilegien werden an eine Datenbankrolle vergeben, die dann an einen Applikationsbenutzer, -rolle vergeben wird.

Datensicherheitskonzepte

- Application Privilege
  - werden an einen Principal vergeben
  - sie werden in einer Sicherheitsklasse vergeben
- Security Class
  - beinhalten Applikationsprivilegen, die auch vererbbar sind.
  - sind typischweise mit ACL‘s versehen. Werden an Principals vergeben.
- Access Control Entry (ACE) ,Teil der ACL
  - Vergibt oder entzieht Applikationsprivilegien einem bestimmten Principal.
- Access Control List (ACL)
  - Liste von Control Einträgen
- Data Security Police
  - Schützt Daten im Row-Level bzw. Column-Level Modus. (Fine grained.)

Oracle Database Real Application Security
- PL/SQL Packages/Functions
- Data Dictionary Views

Oracle Database Real Application Security PL/SQL Packages

PL/SQL Package	Beschreibung
DBMS_XS_SESSIONS	Verwaltung von Application Sessions
XS_ACL	Verwaltung von ACLs
XL_ADMIN_UTIL	Hilfsprogramme
XS_DATA_SECURITY	Verwaltung von Data Security Policies
XS_DATA_SECURITY_UTIL	Hilfsprogramme für statische ACL
XS_DIAG	Problemdiagnose und Reports
XS_NAMESPACE	Verwaltung von Namespaces
XS_PRINCIPAL	Verwaltung von Principals
XS_SECURITY_CLASS	Verwaltung von Data Security Classes

- Java Integration über Package oracle.security.xs
- bereits in APEX integriert.

Oracle Database Real Application Security SQL Functions

PL/SQL Package	Beschreibung
COLUMN_AUTH_INDICATOR	Spaltenauthorisierungsfunktion
XS_SYS_CONTEXT	Session Attribute
ORA_CHECK_ACL	Prüft, ob ein Applikationsbenutzer ein bestimmtes Applikationsrecht besitzt.
ORA_CHECK_PRIVILEGE	Prüft, ob ein Applikationsbenutzer ein bestimmtes Systemrecht besitzt.
ORA_GET_ACLIDS	ACL Identifier Function
TO_ACLID	ACL Identifier Function

Oracle Database Real Application Security Data Dictionary Views

- RAS verwendet die Views DBA_XS_***

View	Beschreibung
DBA_XS_USERS	Real Application Security User
DBA_XS_ROLES	Real Application Security Roles
DBA_XS_SECURITY_CLASSES	Real Application Security Classes
DBA_XS_ACLS	Real Application Security ACLs
DBA_XS_ACL_PARAMETERS	Real Application Security ACL Parameter
DBA_XS_COLUMN_CONSTRAINTS	Real Application Security Column Cons.
DBA_XS_REALM_CONSTRAINTS	Real Application Security Realm Cons.
DBA_XS_POLICIES	Real Application Security Policies
DBA_XS_SECURITY_CLASSES	Real Application Security Classes
…	…

UseCase

Use Case

- Tabelle: PROJECTS

```
SQL> descr projects
 Name                                      Null?    Type
 ----------------------------------------- -------- ----------------------------
 PROJECT_ID                                NOT NULL NUMBER
 PROJECT_NAME                              NOT NULL VARCHAR2(30)
 START_DATE                                         DATE
 END_DATE                                           DATE
 PROJECT_VALUE                                      NUMBER
 PROJECT_OWN                               NOT NULL VARCHAR2(20)
```

- Applikationsbenutzer AKRAFT darf nur Projekte der Abteilung ABT_A lesen aber nicht den Projektwert. Hat keine Schreibrechte.
- Applikationsbenutzer SOEHRLI darf nur Projekte der Abteilung ABT_B lesen inklusive Projektwert und darf Datensätze ändern. Darf aber Datensätze nicht Hinzufügen oder Löschen.

Konfiguration/Komponenten für den UseCase

Principal

- Principal
  - kann ein
    - Applikationsbenutzer,
    - eine Applikationsrolle,
    - ein Datenbankbenuzter,
    - eine Datenbankrolle.

      sein.

```
SQL> REM Applikationsbenutzer anlegen.
SQL> exec sys.xs_principal.create_user(name=>'AKRAFT',schema =>'SCOTT');
SQL> exec sys.xs_principal.set_password(user =>'AKRAFT',password => 'XX');
```

Applicationrole

- Applikationsrollen
  - besteht aus applikationsdefinierten Privilegien sowie deklarativen Access Control Lists (ACL)

```
REM Datenbankrolle
SQL> create role DB_PROJECTS;
SQL> grant select, insert, update, delete on scott.projects to DB_PROJECTS;
REM
REM Applikationsrolle
SQL> exec xs_principal.create_role(name => 'APPL_ABT_A_ROLE', enabled => true);
REM
REM Datenbankrolle an Applikationsrolle vergeben
SQL> grant DB_PROJECTS to APPL_ABT_A_ROLE;
```

Application Users

- können als
  - Direct Login Application User Account (bspw. mit SQL*Plus) arbeiten.

```
SQL> connect akraft/ras1welcome@localhost:1521/pdb4711
Connected.
```

Application Sessions

- werden in zwei Phasen konfiguriert.
  - Anlegen und Erhalten der Application Session.
  - Manipulation der Session während ihrer Dauer.
- werden angelegt mit
  - PL/SQL (**`DBMS_XS_SESSION.CREATE_SESSION`**)
  - Java (**`XSSessionManager Class => Methode createSession)`**
- Vorteile gegenüber traditionellen Datenbank Sessions.
  - erlauben den Applikationen Datenbank Authorisierungsmechanismen.
  - gleichzeitige Verknüpfung von mehreren Datenbanksessions.
  - sind im Oracle RAC Umfeld von allen Knoten zugänglich,
  - weniger Overhead
  - Können Session Änderungen auf dem Client sammlen. (Caches)

Application Sessions

- Beispiel als User: rasadm angemeldet.

```
var gsessionid varchar2(32); -- Attach Session
declare
  sessionid raw(16);
begin
  dbms_xs_sessions.create_session('AKRAFT', sessionid);
 :gsessionid := rawtohex(sessionid);
  dbms_xs_sessions.attach_session(sessionid, null);
end ;
/
```

```
Declare                          -- Detach Session and destroy session
  sessionid raw(16);
begin
  sessionid := hextoraw(:gsessionid);
  dbms_xs_sessions.detach_session;
  dbms_xs_sessions.destroy_session(sessionid);
end;
/
```

Security Class

- vordefinierte Security Classes

```
SQL> SELECT * FROM dba_xa_security_classes;

NAME                 OWNER      DESCRIPTION
-------------------- ---------- ----------------------------------------
DML                  SYS        DML Privileges Security Class
SYSTEM               SYS        System Security Class
ALL                  SYS        All Security Class
SESSION_SC           SYS        Session Security Class
NSTEMPLATE_SC        SYS        Namespace Template Security Class
NETWORK_SC           SYS        Network Security Class
OlapPrivileges       SYS        OLAP Data Security Class
```

Security Class

- eigen erstellte Security Class, benutzt vordefinierte Security Class „DML“.

```
declare
begin
  xs_security_class.create_security_class(
    name        => 'PROJECTS_SC',
    parent_list => xs$name_list('sys.dml'),
    priv_list   => xs$privilege_list(xs$privilege('VIEW_PROJECT_VALUE')));
end;
/
```

ACLs

- Access Control List (ACL)
  - Liste von Control Einträgen

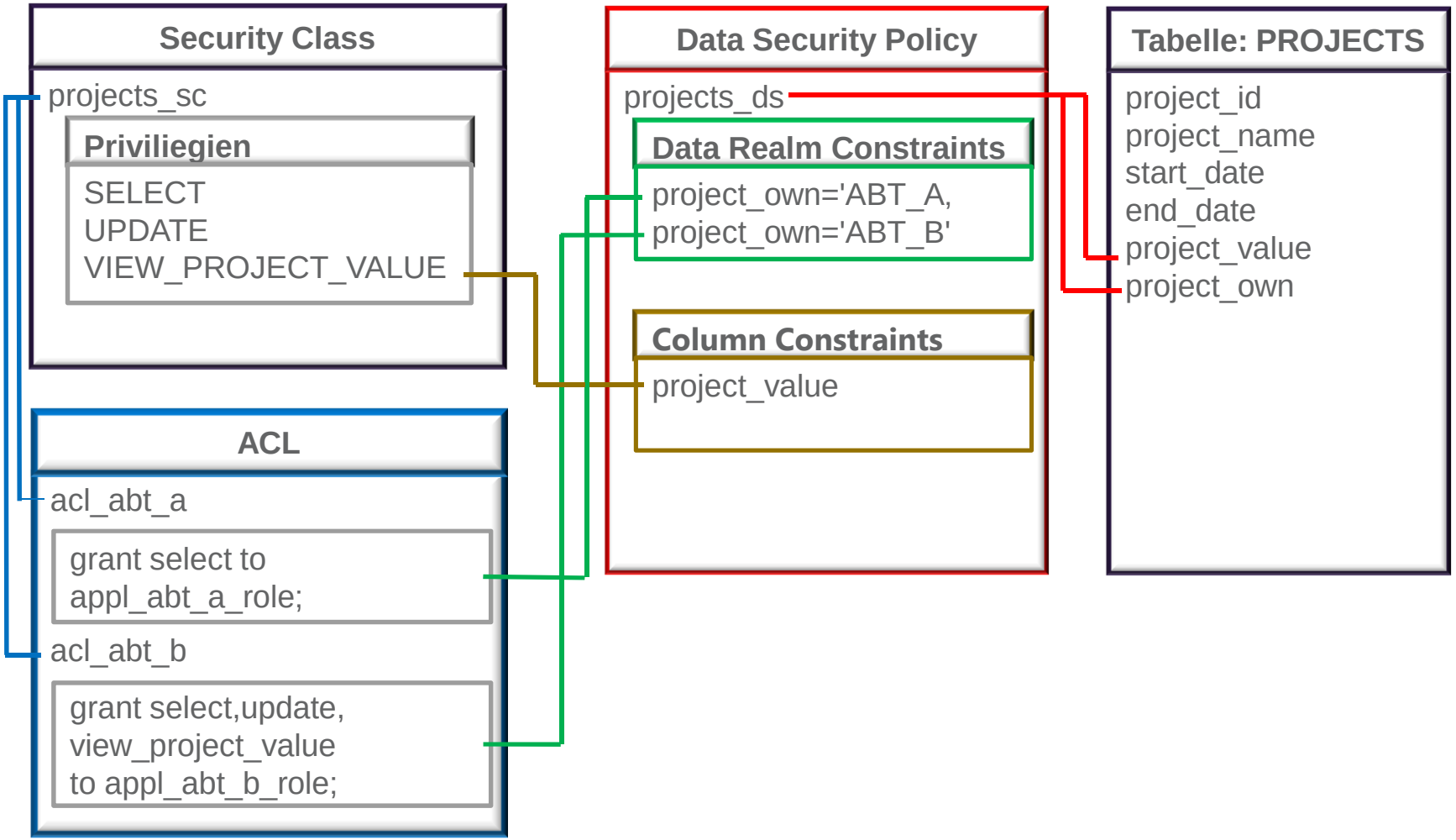
```
declare
  aces xs$ace_list := xs$ace_list();
begin
  aces.extend(1);
  -- SEL_ACL:  nur Lesen.
  aces(1) := xs$ace_type(privilege_list => xs$name_list('SELECT'),
                         principal_name => 'APPL_ABT_A_ROLE');
  xs_acl.create_acl(name      => 'ACL_ABT_A',
                    ace_list  => aces,
                    sec_class => 'PROJECTS_SC');
  aces(1) := xs$ace_type(privilege_list =>
                         xs$name_list('SELECT','UPDATE','VIEW_PROJECT_VALUE'),
                         principal_name => 'APPL_ABT_B_ROLE');
  xs_acl.create_acl(name      => 'ACL_ABT_B',
                    ace_list  => aces,
                    sec_class => 'PROJECTS_SC');
end;
```

Data Security Policy

Data Security Policy

```
declare
  realms   xs$realm_constraint_list := xs$realm_constraint_list();
  cols     xs$column_constraint_list := xs$column_constraint_list();
begin
  realms.extend(2);
  realms(1) := xs$realm_constraint_type(realm    => 'project_own=''ABT_A''',
                                        acl_list => xs$name_list('ACL_ABT_A'));
  realms(2) := xs$realm_constraint_type(realm    => 'project_own=''ABT_B''',
                                        acl_list => xs$name_list('ACL_ABT_B'));
  cols.extend(1);
  cols(1) := xs$column_constraint_type( column_list => xs$list('project_value'),
                                        privilege   => 'VIEW_PROJECT_VALUE');
  xs_data_security.create_policy(name => 'PROJECTS_DS',
                                 realm_constraint_list  => realms,
                                 column_constraint_list => cols);
  xs_data_security.apply_object_policy(policy => 'PROJECTS_DS',
                                       schema => 'SCOTT',
                                       object =>'PROJECTS');
end;
```

Zusammenfassung



Auditing

Audit Policy

- DML-Zugriffe auf die Tabelle PROJECTS mitprotokollieren.

```
SQL> CREATE AUDIT POLICY scott_projects_policy ACTIONS
  2 SELECT ON SCOTT.projects,
  3 INSERT ON SCOTT.projects,
  4 DELETE ON SCOTT.projects,
  5 UPDATE ON SCOTT.projects;
Audit policy created.

SQL> AUDIT POLICY scott_projects_policy;

Audit succeeded.

SQL> SELECT *
   2 FROM    audit_unified_enabled_policies
   3 WHERE   policy_name = 'SCOTT_EMP_DML_POLICYY';

USER_NAME POLICY_NAME           ENABLED_OPT SUCCESS FAILURE
--------- --------------------- ----------- ------- -------
ALL_USERS SCOTT_PROJECTS_POLICY BY          YES     YES
```

Audit Policy

- Abfrage des UNIFIED_AUDIT_TRAIL.
- Zugriffe auf die Tabelle PROJECTS im Schema SCOTT.
- In Spalte XS_USER_NAME steht der Applikationsuser.

```
SQL> SELECT xs_user_name,to_char(event_timestamp,'DD.MM.YYYY HH24:MI:SS')
            Zugriffszeit ,object_name,sql_text
  2  FROM   unified_audit_trail
  3  WHERE  unified_audit_policies='SCOTT_PROJECTS_POLICY';

XS_USER_NAME  ZUGRIFFSZEIT        OBJECT_NAME  SQL_TEXT
------------- ------------------- ------------ ----------------------------
AKRAFT        17.01.2015 15:16:02 PROJECTS     select * from projects
AKRAFT        17.01.2015 15:19:31 PROJECTS     update projects set
                                               project_value=1000
```

Fazit

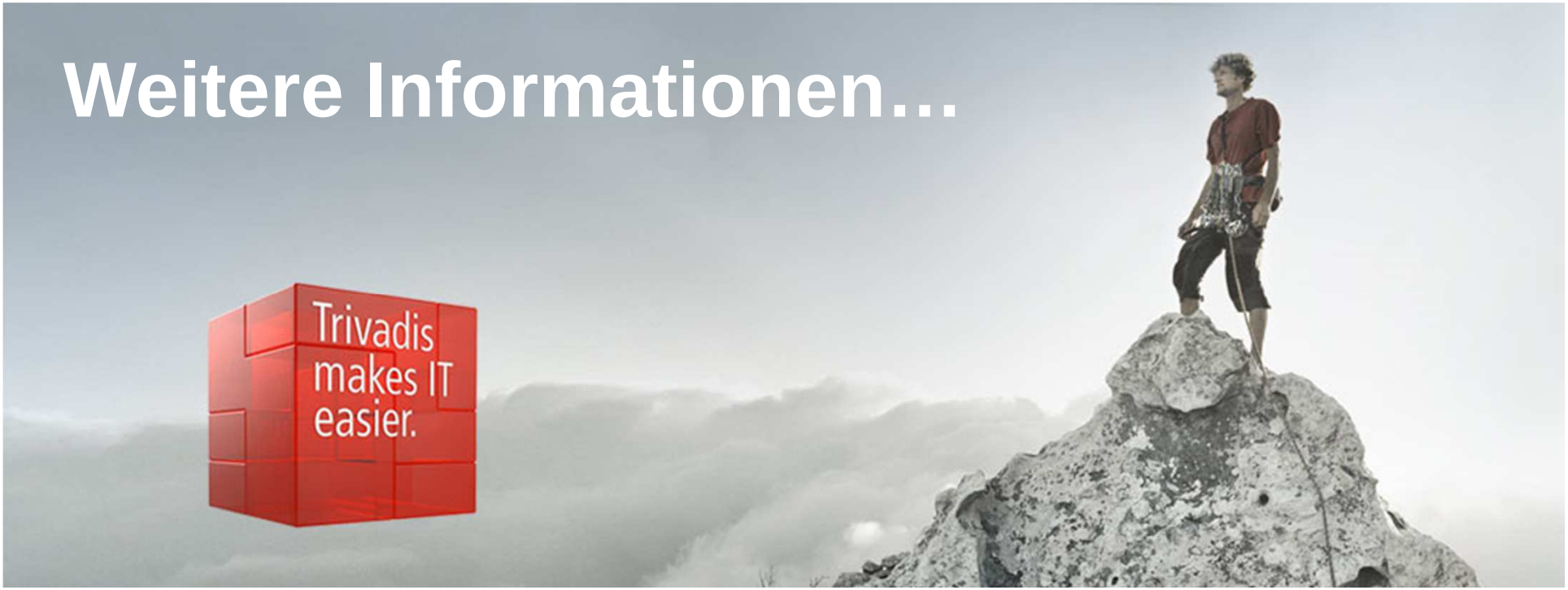
Fazit…

Oracle 12c Real Application Security ist der richtige Ansatz zur Umsetzung von durchgängigen Sicherheitsanforderungen.

Keine Best Practices vorhanden sowie umgesetzte Projekte.

Demo

Weitere Informationen…



- Oracle Dokumentation
  - Oracle® Database Security Guide 12c Release 1 (12.1)
  - Database Real Application Security Administrator's and Developer's Guide 12c Release 1 (12.1)

- Trivadis eXpert Team Security

  http://www.trivadis.com/de/security

trivadis
makes IT easier.

Fragen und Antworten

Axel Kraft
Senior Consultant

Tel. +49 711 903 63 230
axel.kraft@trivadis.com

trivadis
makes IT easier.