

Wie sicher ist die Datenbank vorm Administrator?



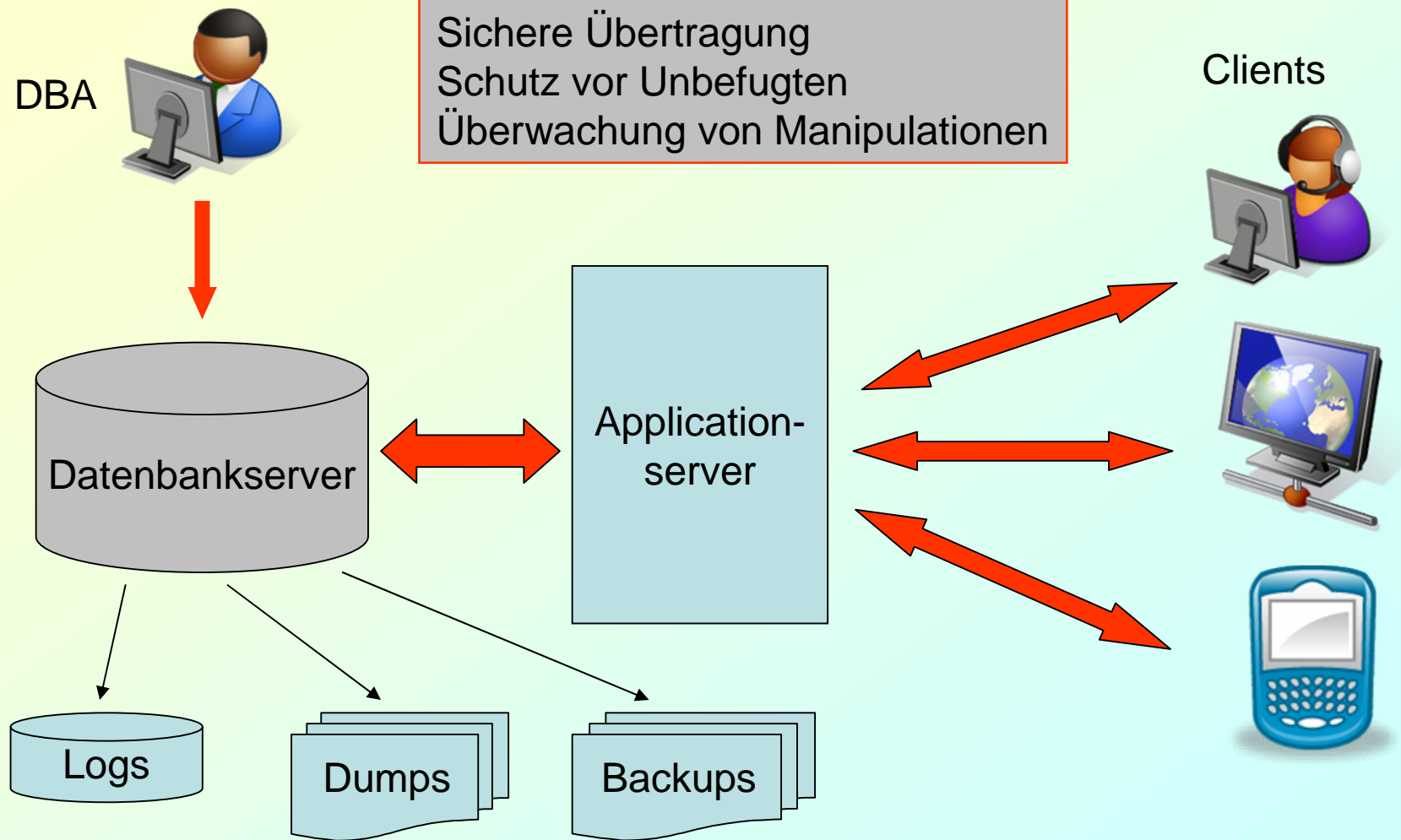
Nürnberg, 19.11.2009

Dr. Frank Haney

Inhalt

- Ø Sicherheit wovor?
- Ø Oracle-Sicherheits-Features im Überblick
- Ø Transparent Data Encryption
- Ø Auditing
- Ø Oracle Database Vault – Übersicht
- Ø Rechtliche Regelungen und Database Vault
- Ø Database Vault – Komponenten
 - Sicherheitsbereiche
 - Trennung der Verantwortlichkeiten
 - Multifaktorielle Zugriffskontrolle
 - Kommandobasierte Sicherheitsregeln
 - Berichte über sicherheitsrelevante Zugriffe
- Ø Die Administrationsoberfläche DVA
- Ø Beispiele

Sicherheit der Daten – Herausforderungen



Security – Oracle Features

- Ø **Standardauthentifizierung** – Paßwortsicherheit durch Profile
- Ø **Standardautorisierung** – Rechtevergabe und Rollen
- Ø **Standardauditing** – Überwachung auf den Ebenen
Schemaobjekt, SQL-Anweisung und Privilegienbenutzung
- Ø **Virtual Private Database (VPD)** – Personalisierung der
Information
- Ø **Secure External Password Store** – Paßwortspeicherung in
Wallets
- Ø **Proxy Authentication** – Authentifizierung des Client-Users
bei der Datenbank in Multi-Tier-Architekturen
- Ø **Secure Application Roles** – Schutz der Rollen durch eine
Policy
- Ø **Fine Grained Auditing (FGA)** – Überwachung des
Datenzugriffs auf Zeilen- und Spaltenebene

Security – Optionen

Ø Oracle Advanced Security

- Transparent Data Encryption (TDE) für
 - Spalten
 - Tablespaces (11g)
 - RMAN Backupsets
 - Datapump
 - Secure Files (11g)
 - Logminer (11g) → Oracle Streams und Logical Standby
- Netzwerkverschlüsselung mit SSL
- Starke Authentifizierung mit Kerberos and PKI

Ø Oracle Label Security

- Zugriffskontrolle auf Zeilenebene

Ø Database Vault (im Vortrag)

Ø Data Masking

- Maskierung der Echtdaten in nichtproduktiven Umgebungen

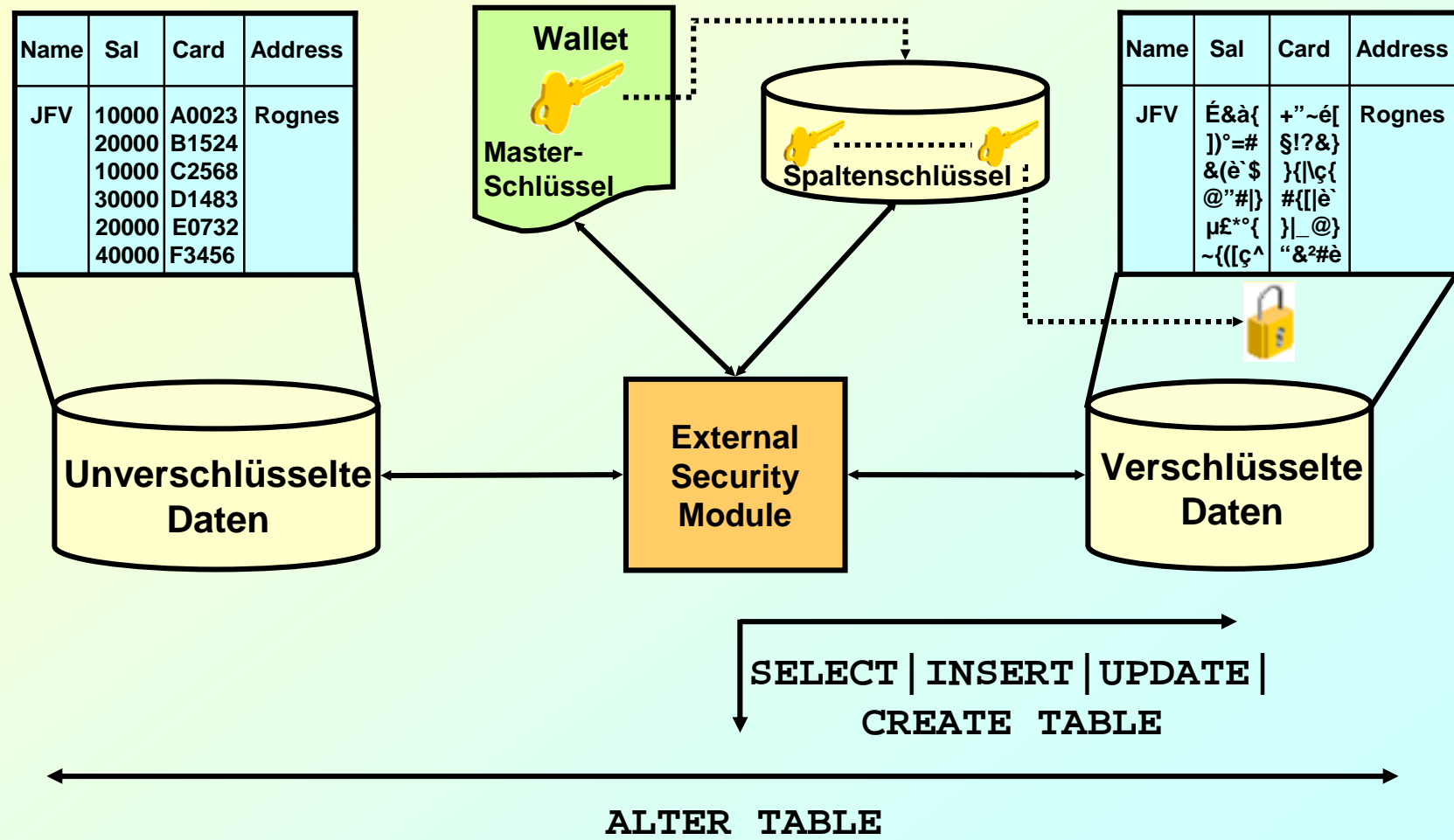
Ø Identity Management (Separates Produkt – früher OID)

- Unternehmensweites Identity Management

Ø Oracle Audit Vault (Separates Produkt)

- Unternehmensweite Konsolidierung des Auditing
- Speicherung der Audit Trails für alle Datenbanken in einem einheitlichen Repository

Transparent Data Encryption - Spalten



TDE – Ablauf

1. Wallet anlegen (automatisch sqlnet.ora oder durch Wallet Manager)

```
ENCRYPTION_WALLET_LOCATION = (SOURCE = (METHOD = FILE)  
                               (METHOD_DATA = (DIRECTORY = ...)))
```

2. Masterschlüssel festlegen

```
ALTER SYSTEM SET ENCRYPTION KEY IDENTIFIED BY <password>;
```

3. Wallet öffnen

```
ALTER SYSTEM SET ENCRYPTION WALLET OPEN IDENTIFIED BY  
<password>;
```

4. Spalten verschlüsseln

```
CREATE TABLE mitarbeiter (  
    name          VARCHAR2(128),  
    vorname       VARCHAR2(128),  
    mitID         NUMBER ENCRYPT NO SALT,  
    gehalt        NUMBER(6) ENCRYPT USING '3DES168',  
    provision     NUMBER(6) ENCRYPT);
```

Überwachung von Datenbankaktionen

Auditing ist die Überwachung und Aufzeichnung von ausgewählten Datenbankaktionen bezüglich

- Ausgeführter SQL-Statements
- Genutzter Privilegien
- Objektzugriff

Mit dem statischen Parameter **AUDIT_TRAIL** kann bestimmt werden, wohin die Informationen geschrieben werden:

- none: Auditing ausgeschaltet (Default)
- os: Audits werden in das Betriebssystem geschrieben.
- db: Audits werden in Datenbanktabellen geschrieben
- db, extended: zusätzlich SQL-Text und Binds
- xml: XML-Dateien im Betriebssystem
- xml, extended: zusätzlich SQL-Text und Binds

Informationen können bei Auditing in die Datenbank mit der View **DBA_AUDIT_TRAIL** abgefragt werden.

Auditing – Syntax

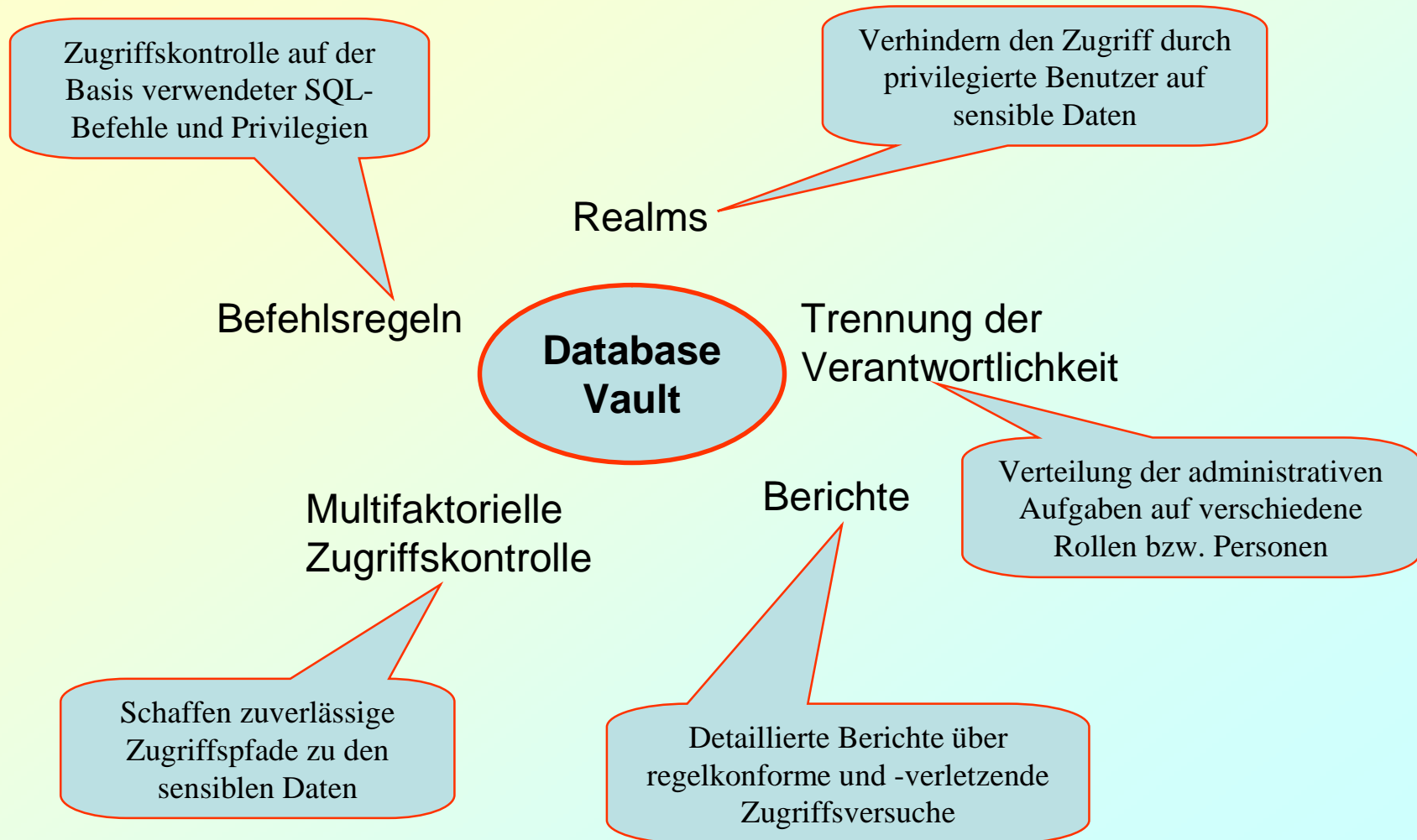
```
AUDIT { sql_statement_clause | schema_object_clause |  
NETWORK }  
[ BY { SESSION | ACCESS } ] [ WHENEVER [ NOT ]  
SUCCESSFUL ];
```

```
sql_statement_clause ::= { statement_option | ALL } |  
{ system_privilege | ALL PRIVILEGES }  
[ BY { proxy [, ... ] | user [, ... ] } ]
```

```
schema_object_clause ::= { object_option [, ... ] | ALL }  
auditing_on_clause
```

```
auditing_on_clause ::= ON { [ schema.]object |  
DIRECTORY directory_name | DEFAULT }
```

Database Vault – Übersicht



Gesetzliche Regelungen und Database Vault

Ausgewählte Gesetze und Standards:

- Ø Sarbanes-Oxley
- Ø Gramm-Leach-Bliley
- Ø Basel II – Internal Risk Management
- Ø PCI DSS (Payment Card Industry Data Security Standard)
- Ø Japan Privacy Law

Forderungen von **PCI DSS**, denen Database Vault genügt:

- Ø Zugriff auf Kreditkartendaten nur für autorisierte Nutzer
- Ø Beschränkung von Wartungsmaßnahmen auf bestimmte Zeitfenster
- Ø Datenzugriff eingeschränkt auf definierte
 - IP- und Mac-Adresse
 - Applikation bzw. Service
 - Benutzer-Accounts und –gruppen
- Ø Jede Einheit darf nur Zugang zu den Kreditkartendaten der „eigenen“ Kunden haben (Mandantentrennung)

Database Vault – Grundlagen

∅ Voraussetzungen

- Datenbank mindestens 9.2.0.8
- Label Security installiert (optional)
- Enterprise Manager Database Control installiert und konfiguriert

∅ Geänderte Standardeinstellungen z.B.

- Geänderte Initialisierungsparameter: `AUDIT_SYS_OPERATIONS=TRUE` und nicht mehr `FALSE`
- Der User `SYS` hat keine Recht auf `ALTER SESSION` mehr.
- Das Package `DBMS_RLS` (Label Security) gehört jetzt dem Database Vault Administrator
- `EXECUTE` auf `UTL_FILE` nicht mehr an `PUBLIC` vergeben

∅ Neue Schemata

- `DVSYs`: Eigentümer des Oracle Database Vault Schemas
- `DVF`: Eigentümer der Oracle Database Vault Faktorfunktionen

Trennung der Verantwortlichkeiten

∅ Neue Rollen

- DV_OWNER: Oracle Database Vault Owner Role
- DV_REALM_OWNER: Oracle Database Vault Realm DBA Role
- DV_REALM_RESOURCE: Oracle Database Vault Application Resource Owner Role
- DV_ADMIN: Oracle Database Vault Configuration Administrator Role
- DV_ACCTMGR: Oracle Database Vault Account Manager Role
- DV_SECANALYST: Oracle Database Vault Security Analyst Role
- DV_PUBLIC: Oracle Database Vault PUBLIC Role

∅ Vertrauenswürdige Accounts

- DV_ACCTMGR role
- DV_OWNER role
- SYSDBA privilege
- SYSOPER privilege

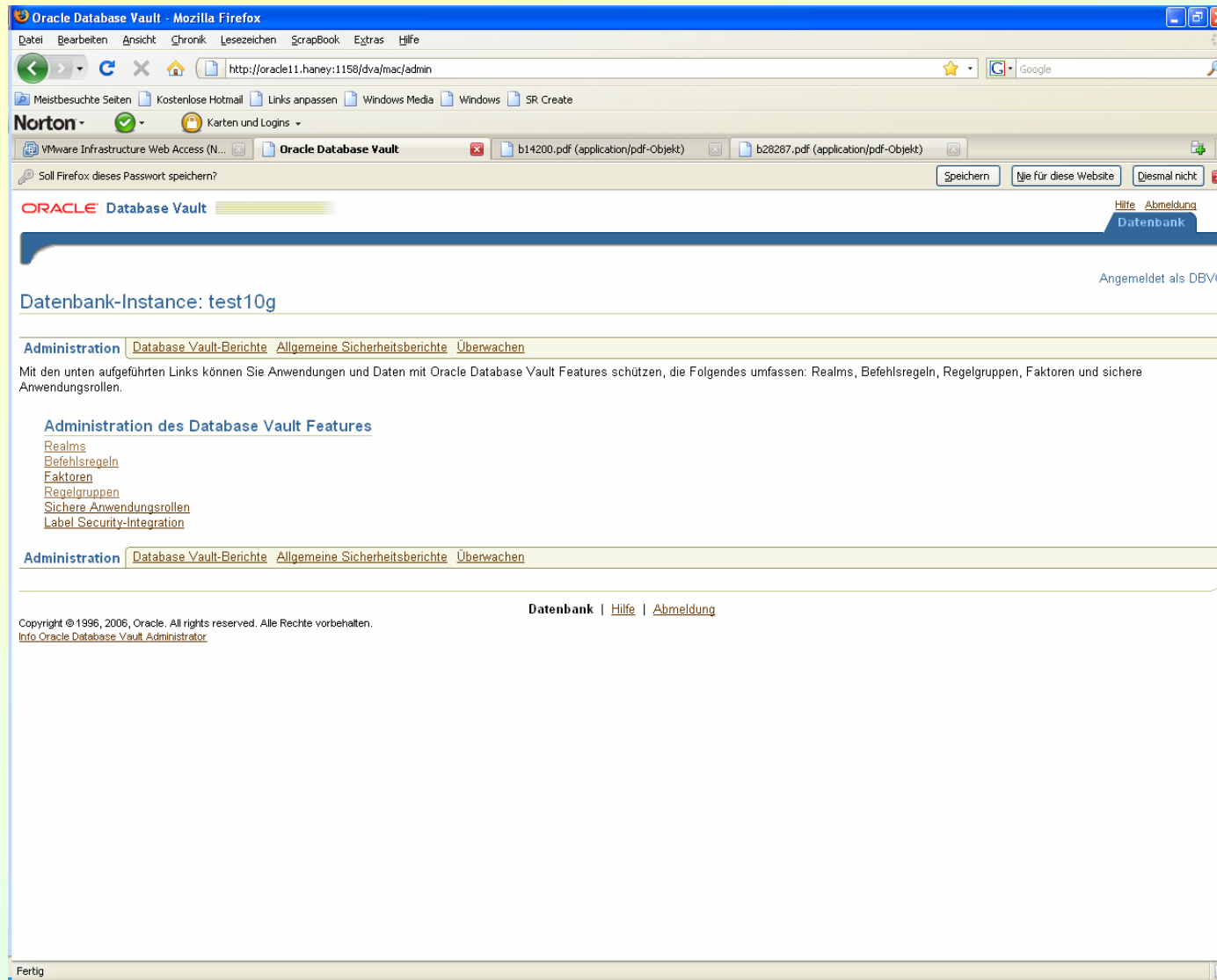
∅ Accounts und Rollen nur an vertrauenswürdige Individuen vergeben

- User mit Root-Zugriff auf das Betriebssystem
- Eigentümer der Oracle Software
- SYSDBA-Zugriff
- SYSOPER-Zugriff

Sicherheitsrichtlinien im Umfeld von Database Vault

1. Zugriff auf die Packages UTL_FILE und DBMS_FILE_TRANSFER begrenzen
2. Eingeschränkter Zugriff auf den Recycle Bin
3. Besondere Vorsicht beim Umgang mit den Privilegien CREATE ANY JOB and CREATE JOB
4. Vorsicht beim Privileg CREATE EXTERNAL JOB
5. Unbedingt den Zugriff auf das Package LogMiner beschränken
6. Die Verwendung der Privilegien ALTER SYSTEM und ALTER SESSION beschränken
7. Vorsicht mit Java Stored Procedures
8. Vorsicht bei externen C-Programmen in der Datenbank

Administration mit dem DVA



Sicherheitsbereiche (Realms) im DVA

The screenshot shows the Oracle Database Vault Administration interface in a Mozilla Firefox browser. The page title is "Oracle Database Vault" and the URL is "http://oracle11.haney:1158/dva/mac/admin/realm". The page displays the "Realms" section for the instance "test10g". A table lists five realms with their respective audit options and security settings.

Datenbank-Instance: test10g > Realms Angemeldet als DBVO

Realms

Mit Database Vault Realms können Datenbankschemas und Datenbankrollen in funktionalen Gruppen klassifiziert werden, um eine fein granulierte Access Control für die Verwendung von Berechtigungen auf Systemebene für diese Typen von Datenbankobjekten bereitzustellen.

[Erstellen](#) [Bearbeiten](#) [Entfernen](#)

Auswählen	Name ▲	Audit-Optionen	Oracle-definierte Realm?	Objekte geschützt?	Benutzer autorisiert?	Status
<input checked="" type="radio"/>	Database Vault Account-Management	Audit bei Fehler	✓	✓	✓	✓
<input type="radio"/>	Oracle Data Dictionary	Audit bei Fehler	✓	✓	✓	✓
<input type="radio"/>	Oracle Database Vault	Audit bei Fehler	✓	✓	✓	✓
<input type="radio"/>	Oracle Enterprise Manager	Audit bei Fehler	✓	✓	✓	✓
<input type="radio"/>	TEST_R_HR	Audit bei Erfolg oder Fehler		✓	✓	✓

[Bearbeiten](#) [Entfernen](#)

Datenbank | [Hilfe](#) | [Abmeldung](#)

Copyright © 1996, 2006, Oracle. All rights reserved. Alle Rechte vorbehalten.
[Info Oracle Database Vault Administrator](#)

Fertig

Befehlsregeln im DVA

The screenshot shows the Oracle Database Vault Administration interface in a Mozilla Firefox browser. The page title is "Oracle Database Vault" and the URL is "http://oracle11.haney:1158/dva/mac/admin/command". The page is titled "Befehlsregeln" (Command Rules) for the database instance "test10g". It explains that command rules control the execution of DDL commands and database operations. A table lists various SQL commands, their owners, object names, rule group names, and their status. The "SELECT" command is marked with a red 'x' in the status column, indicating it is not allowed. The page includes navigation buttons for "Erstellen", "Bearbeiten", and "Entfernen".

Datenbank-Instance: test10g > Befehlsregeln Angemeldet als DBVO

Befehlsregeln

Befehlsregeln kontrollieren die Möglichkeit, Data Definition Language-(DDL-)Befehle und besondere Datenbankvorgänge zu verarbeiten. Befehlsregeln bestimmen, ob der Befehl je nach Auswertung einer Database Vault-Regelgruppe erfolgreich verlaufen darf.

[Erstellen](#)

[Bearbeiten](#) [Entfernen](#)

Auswählen	Befehl	Objekteigentümer	Objektname	Name der Regelgruppe	Status
<input checked="" type="radio"/>	ALTER PROFILE	%	%	Kann Accounts/Profile verwalten	✓
<input type="radio"/>	ALTER SYSTEM	%	%	Systemparameter zulassen	✓
<input type="radio"/>	ALTER USER	%	%	Kann eigenen Account verwalten	✓
<input type="radio"/>	CREATE PROFILE	%	%	Kann Accounts/Profile verwalten	✓
<input type="radio"/>	CREATE USER	%	%	Kann Accounts/Profile verwalten	✓
<input type="radio"/>	DROP PROFILE	%	%	Kann Accounts/Profile verwalten	✓
<input type="radio"/>	DROP USER	%	%	Kann Accounts/Profile verwalten	✓
<input type="radio"/>	ALTER TABLE	SCOTT	%	ALTER TABLE Security Policy	✓
<input type="radio"/>	SELECT	SCOTT	EMP	ALTER TABLE Security Policy	✗
<input type="radio"/>	GRANT	SYS	DBMS_RLS	Kann VPD-Administration erteilen	✓
<input type="radio"/>	REVOKE	SYS	DBMS_RLS	Kann VPD-Administration erteilen	✓

[Bearbeiten](#) [Entfernen](#)

Datenbank | [Hilfe](#) | [Abmeldung](#)

Copyright © 1996, 2006, Oracle. All rights reserved. Alle Rechte vorbehalten.
[Info Oracle Database Vault Administrator](#)

Fertig

Sicherheitsberichte

Oracle Database Vault - Mozilla Firefox

http://oracle11.haney:1158/dva/mac/report

ORACLE Database Vault

Hilfe Abmeldung Datenbank

Angemeldet als DBVO

Datenbank-Instance: test10g

Administration Database Vault-Berichte Allgemeine Sicherheitsberichte Überwachen

Verwenden Sie diesen Bildschirm zur Ausführung von Berichten über potenzielle Database Vault-Konfigurationsprobleme und Database Vault Audit-Ereignisse.

Bericht ausführen

Alle einblenden | Alle ausblenden

Berichte

Auswählen Fokus Berichtstitel:

		Berichtstitel
<input type="radio"/>		▼ Berichte
<input type="radio"/>	⊕	▼ Berichte über Database Vault-Konfigurationsprobleme
<input checked="" type="radio"/>		Probleme bei Befehlsregelkonfiguration
<input type="radio"/>		Probleme bei Faktorkonfiguration
<input type="radio"/>		Faktoren ohne Identitäts
<input type="radio"/>		Identity-Konfigurationsprobleme
<input type="radio"/>		Probleme bei Realm-Autorisierungskonfiguration
<input type="radio"/>		Probleme bei Regelgruppenkonfiguration
<input type="radio"/>		Probleme bei Konfiguration von sicheren Anwendungen
<input type="radio"/>	⊕	▼ Berichte über Database Vault Auditing
<input type="radio"/>		Realm Audit
<input type="radio"/>		Befehlsregel-Audit
<input type="radio"/>		Faktor-Audit
<input type="radio"/>		Audit von Label Security-Integration
<input type="radio"/>		Audit Trail von Core Database Vault
<input type="radio"/>		Audit von sicherer Anwendungsrolle

Bericht ausführen

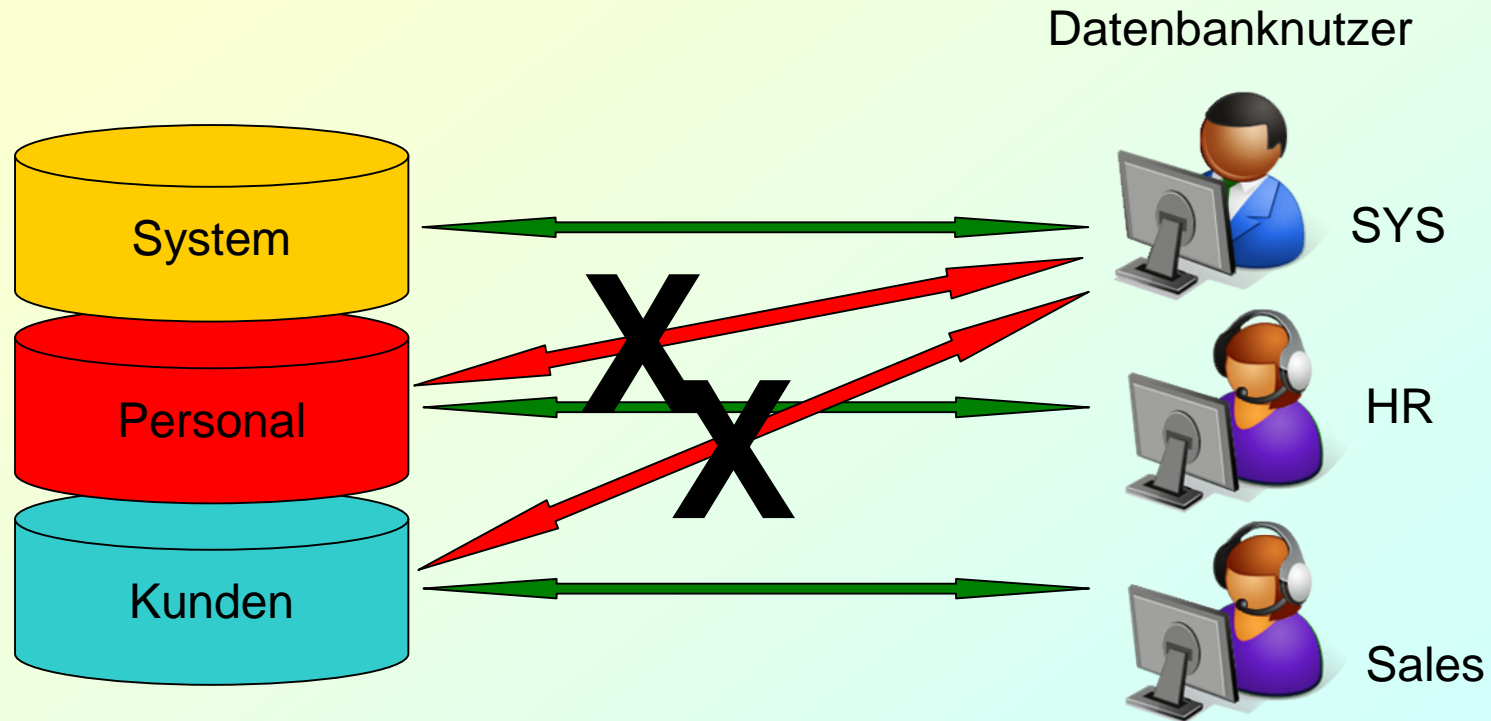
Administration Database Vault-Berichte Allgemeine Sicherheitsberichte Überwachen

Datenbank | Hilfe | Abmeldung

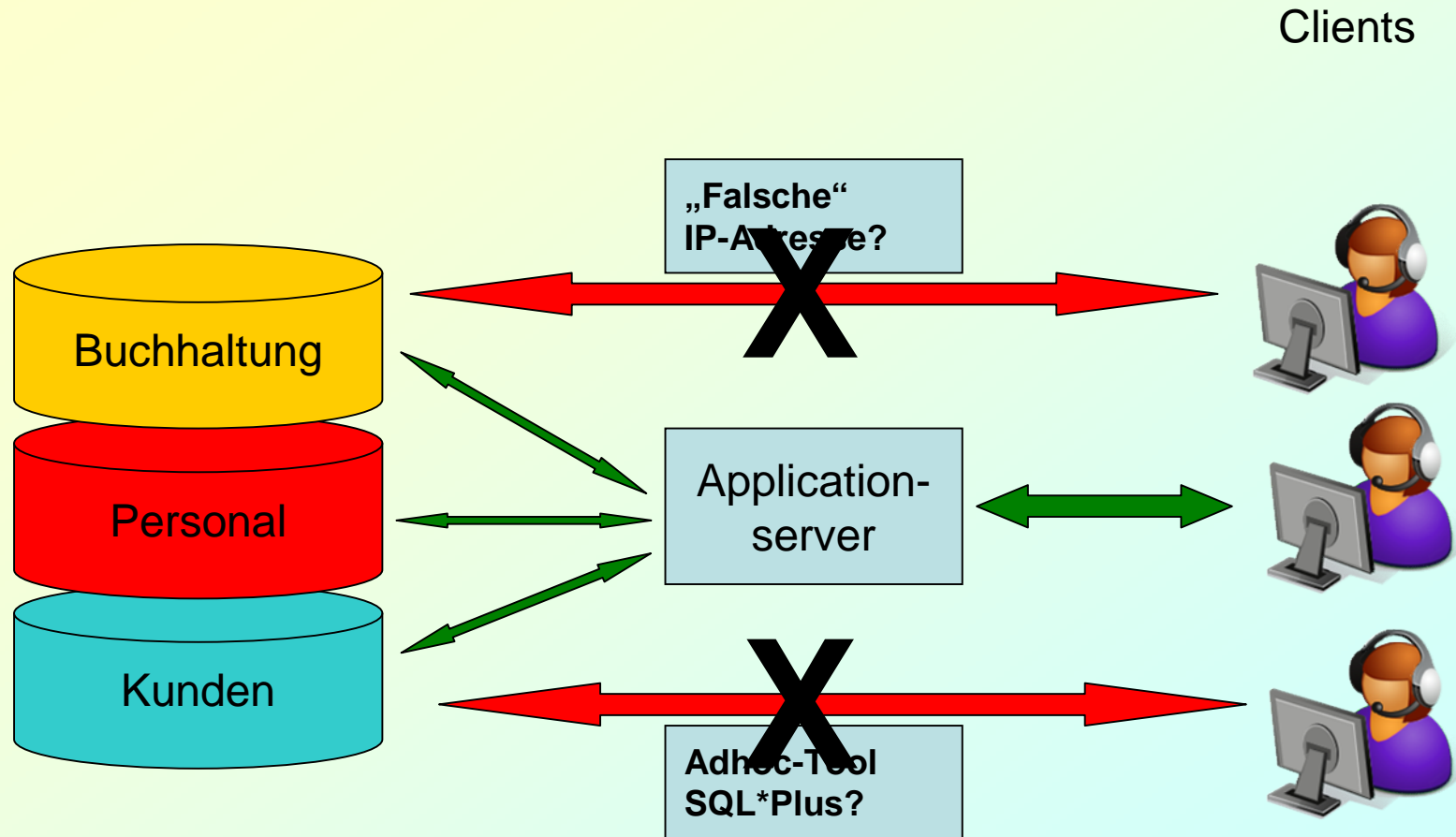
Copyright © 1996, 2006, Oracle. All rights reserved. Alle Rechte vorbehalten.
Info Oracle Database Vault Administrator

Fertig

Oracle Database Vault Realms



Command Rules und multifaktorielle Authorisierung



Neu in Version 11 Release 2

1. Integration in den Enterprise Manager (Database Control 11.2 und Grid Control 10.2.0.5)
2. Unterstützung von Datapump
3. Unterstützung des Schedulers (Scheduler Jobs)
4. Neue Database Vault Rollen
5. Zusätzliche Standard Rule Sets
6. RMAN-Unterstützung
7. Stärkerer Schutz des Schemas DVSYS
8. Neue Standardeinstellungen, z.B. RECYCLEBIN jetzt OFF

Literatur

- Ø OTN <http://www.oracle.com/technology/deploy/security/database-security/>
 - ~/maximum-security-architecture.html
 - ~/oracle-pci.html
 - ~/advanced-security/index.html
- Ø Oracle11g Database Online Documentation Release 2 und 10g Release 2, vor allem folgende Teile:
 - Database Vault Administrator's Guide
 - Security Guide
 - Advanced Security Administrator's Guide

Dr. Frank Haney
info@it-haney.de
Tel.: 03641-210224

