Data Redaction live

Tobias Bräutigam
syntegris information solutions GmbH
Neu-Isenburg

Mike Schliephorst
Selbstständig

Schlüsselworte
Oracle Data Redation, Security, Data Leakage Prevention

Einleitung
Dieser Vortrag ist ein Projektbericht über die erfolgreiche Implementierung von Oracle Data Redaction in einem unternehmenskritischen Datenbanksystem zur Verwaltung von sensibler Daten.
Von der Vision bis zum erfolgreichen Wirkbetrieb berichten wir über die typischen Herausforderungen, überraschenden Lösungen und Anekdoten rund um die Implementierung von Data Redaction in einer über die Jahre gewachsenen Anwendung mit 500.000+ PL/SQL Codezeilen Geschäftslogik.

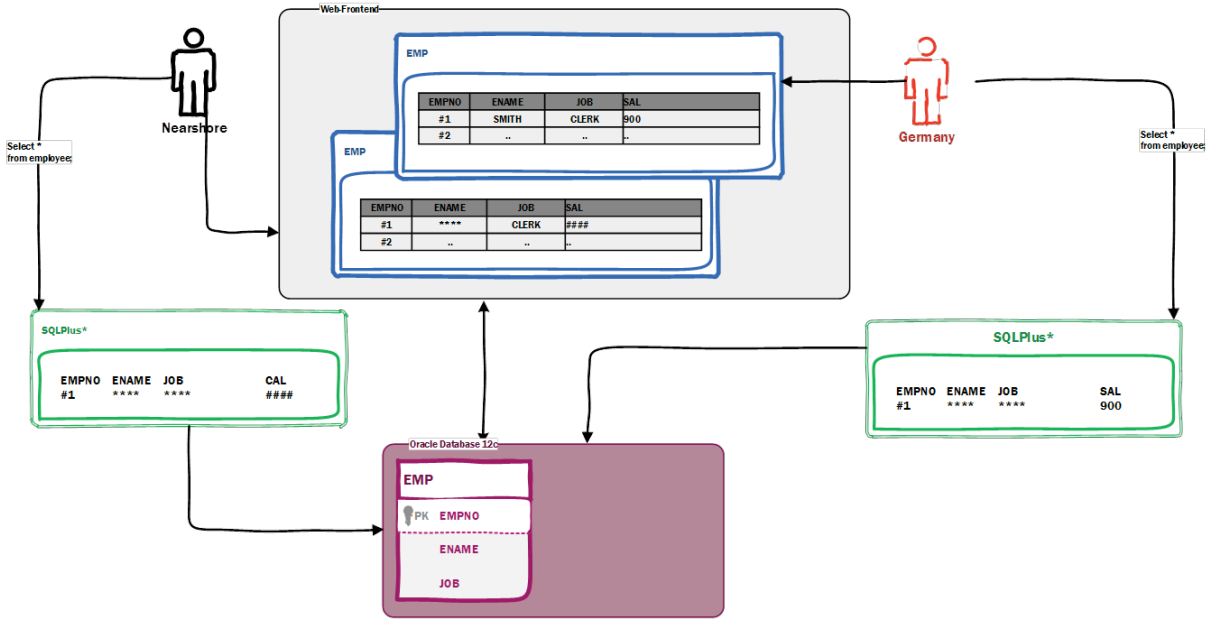

Abb. 1: Architektur, vereinfacht

Anforderungen des Kunden
Zugriff auf sensible Daten durch Nearshore Mitarbeiter

- über Webfrontend mit Internet Explorer
- mit SQL*Plus
- Maskierung direkt in der Datenbank
- Sicherheitskonzept ist Liefergegenstand

Fachlichkeit
Welche Spalten/Felder müssen redaktioniert werden?
Methoden:

- semantische Analyse
- Typanalyse
- Data Dictionary
- CRUD-Matrix (TOAD) aller Tabellen
- Zirkelbezüge in SPs erschweren Analyse

Proof of Concept

- Use Case nur Lesezugriff, einige Frontend-Seiten
- Testfälle erstellen
- System- und Code-Analyse
- Struktur der Codebasis, Konventionen
- Semantik interner Schnittstellen
- Kommentare, Versionierung, Logging
- Muss bestehender Code angepasst werden?
- Lösung auch für direkten SQL-Zugriff geeignet?

Proof of Concept fachlich

Zugriffe der Webapplikation und Seiteneffekte

- Schreibt der Webclient nur tatsächlich geänderte Daten zurück?
- Unbeabsichtigtes Schreiben maskierter Inhalte?
- Gleichzeitige Bearbeitung einer Datensatzes durch Benutzer mit verschiedenen Rollen?

Logische Konsistenz von Daten und Prozessen

- Sind maskierte Spalten und Felder Schlüssel oder logische Schalter?
- Statische Maskierung oder Pseudonymisierung ?

Performance

- Ausführungspläne, Speicherbedarf und Latenzen stabil?

Was genau ist Oracle Data Redaction?

- deklaratives Maskieren bestimmter Spalten-Inhalte
- geeignet zur Anpassung von Datenbank-Applikationen
- Ausführung in der DB zur Laufzeit (11gR2/12c)

Sicherheit

- Häufiges Problem: Datenlecks durch Inferenz
- geeignet für auf der Datenbank aufsetzende Applikationen
- andere Szenarien erfordern zusätzliche Sicherheitsmaßnahmen
- Data Redaction ist per default deaktiviert für `SYS` und `SYSTEM` sowie Export-User
- Privilege
  `EXEMPT REDACTION POLICY`

Einschränkungen

- `INSERT AS SELECT`
- Inferenz DEMO 1
- Doku auf Oracle.com
- von uns entdeckter Oracle Bug und Bugfix

Grenzen und Möglichkeiten

- konzeptionelle Grenzen
- geeignet für Frontend-Zugriffe
- kein Schutz gegen fortgeschrittene Angriffe

Schreibzugriff sicher realisieren

- Date Redaktion und Row Level Security
- Data Redaction behandelt Lesezugriff
- Schreibzugriffe zuverlässig mit RLS absichern
- DEMO 2

Typische Fehlercodes und Überraschungen

- "Poisoned queries" in Legacy Code
- Beispiel
- DEMO 3

Fassadenarchitektur

Data Redaction und RLS Policies, Views, Synonyme und Infrastrukturcode werden hinter einer Facade verkapselt

- logische Trennung
- definierte Zugriffspfade je nach Berechtigung
- Central Enforcement Point

Redaction Policies generieren
DEMO 4

Delta aller Daten in Sekunden

- Datendelta (Diff) der gesamten Datenbank mit Flashback Database in Sekunden erzeugen
- Performance-Probleme, wo?

Erfolgsfaktoren und Fazit

- Fachlichkeit radikal eingrenzen
- Testdaten frühzeitig einfordern
- mehrere Designalternativen bereithalten
- komplementäre Testverfahren
- Entwicklung in Umgebung beim Kunden
- kontinuierliches Deployment
- Projektentscheidungen dokumentieren (+-)

Lieblingstools

One more thing, unsere Lieblingstools

- TOAD, SQLDeveloper, Jmeter
- JIRA – unser Data Dictionary
- Screenpresso, VirtualBox

And yours?

Fragen? Antworten!

Danke!

Kontaktadresse:
Tobias Bräutigam
syntegris information solutions GmbH
Hermannstrasse 54-56
Neu-Isenburg in Hessen

Telefon:	+49 (0) 12-345 6789
Fax:	+49 (0) 12-345 6788
E-Mail	tobias.braeutigam@syntegris.de
Internet:	www.syntegris.de