

In Data-Warehouse-Systemen kommen meist Komponenten verschiedener Software-Hersteller zum Einsatz. Dieser Artikel beschreibt das Zusammenspiel zwischen Oracle und SAS im Bereich der Legitimation, insbesondere, wie die technischen und fachlichen Anforderungen zur benutzerspezifischen Beschränkung der Datenzugriffe umgesetzt werden. Die Anforderungen basieren auf den Erfahrungen aus einem Projekt, in dem eine Oracle-Datenbank zur Datenhaltung und die BI-Lösung von SAS für die Auswertungen und Analysen zum Einsatz kommen.

Zusammenspiel von SAS und Oracle beim Steuern von Datenzugriffen

Christian Schütze, metafinanz-Informationssysteme GmbH

Das Prinzip ist einfach: Anwender in verschiedenen Themengebieten (Sales, Human Resources, Produktion etc.) nutzen eine gemeinsame SAS-Umgebung für Auswertungen und Analysen. Im Infobereich findet man weitere Informationen zu den verwendeten SAS-Komponenten. Die Datenhaltung erfolgt ausschließlich in einer Oracle-Datenbank in Form verschiedener Stern-Schemata (siehe Abbildung 1). Diese enthalten Fakten, Mess-Größen und Kennzahlen, Dimensionen und Merkmale, nach denen Fakten gruppiert werden (siehe Abbildung 2).

In der Fakten-Tabelle „F_ORDERS“ sind verschiedene Kennzahlen enthalten:

- ORDER QUANTITY
- ORDER SALES PRICE
- PRODUCT PRODUCTION COSTS

Der Datenbank-Zugriff erfolgt für eine überschaubare Anzahl von Power-Usern über ein persönliches Login auf die Datenbank. Diese Benutzer können zusätzlich SQL-Abfragen erstellen, deren Zugriff auf die Oracle-Tabellen durch Festlegungen der Daten-Eigentümer eingeschränkt ist. Die Berechtigungen auf die Datenbank-Objekte werden über Oracle-Rollen gesteuert, die gemäß den Themengebieten definiert sind. Der Daten-Eigentümer hat die Möglichkeit, in einer Excel-Datei für jedes Datenbank-Objekt Lesezugriffe durch die Oracle-Rollen anzugeben. Diese Informationen werden von der IT in die Datenbank übernommen. Die Anwender mit einem persönlichen

Datenbank-Login werden einer oder mehreren Oracle-Rollen zugeordnet.

Der Datenbank-Zugriff aus SAS erfolgt für alle Anwender über einen einzigen technischen User. Das reduziert den Administrationsaufwand, weil eine umfangreiche Benutzerverwaltung nur in SAS notwendig ist. Der technische User hat generell Zugriff auf alle Oracle-Tabellen. Es ist also notwendig, in SAS den Zugriff je Themengebiet zu steuern. Dazu sind je Themengebiet Ordner definiert, deren Zugriff mittels SAS-Rolle abgesichert wird. Jede Tabelle, die in SAS verwendet werden soll, muss in SAS registriert sein. Andernfalls ist sie unbekannt und bleibt unsichtbar. Die registrierten Tabellen werden in den jeweiligen Ordnern in SAS abgelegt.

Die Dimensions-Tabellen wurden gemeinsam in einem Ordner abgelegt, auf den es keine Zugriffsbeschränkung gibt. Die Anwender besitzen ein SAS-Login und sind – je nach Themenge-

biet – einer SAS-Rolle zugeordnet. Die Dimension „ORGANIZATION“ enthält eine Hierarchie aus „REGION“ und „COUNTRY“. Jeder Anwender soll eine individuelle und flexibel zu definierende Sicht auf die Daten der „ORGANIZATION“ erhalten (siehe Abbildung 3). Bestimmte Anwender können somit in ihren Auswertungen auf Regionen wie Europa, einzelne Länder wie Deutschland oder beliebige Kombinationen aus Regionen und Ländern beschränkt werden.

In Auswertungen der Anwender soll diese individuelle Dimension verwendet werden. Um dies zu realisieren, wurde für jede Ausprägung der Hierarchie („REGION“ und „COUNTRY“) jeweils eine SAS-Rolle definiert. Die Anwender sind einer oder mehreren dieser SAS-Rollen zugeordnet.

Für die Anbindung in den Auswertungen der Anwender wird in Oracle eine eigene Dimension „SAS_ORGA-

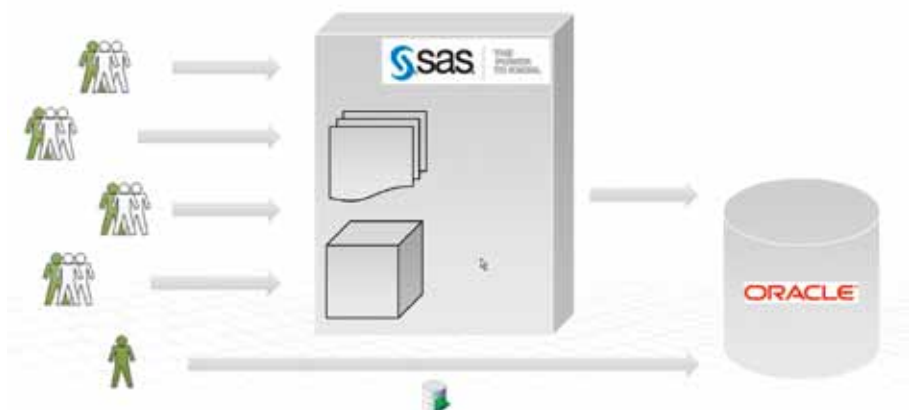


Abbildung 1: System-Architektur mit SAS und Oracle

```
DBMS_RLS.ADD_POLICY(
object_schema => 'SASUSER',
object_name   => 'SAS_ORGANIZATION',
policy_name   => 'POL_ORGANIZATION',
function_schema => 'SASUSER',
policy_function => 'F_AUTH_ORGANIZATION',
statement_types => 'SELECT',
update_check   => false,
enable        => true,
static_policy  => false
);
```

Listing 1

```
DBMS_RLS.ADD_POLICY(
object_schema => 'SASUSER',
object_name   => 'F_ORDERS',
policy_name   => 'POL_HIDE_COLUMNS',
function_schema => 'SASUSER',
policy_function => 'F_AUTH_COLUMNS',
sec_relevant_cols => 'PRODUCT_PRODUCTION_COSTS',
sec_relevant_cols_opt => dbms_rls.ALL_ROWS
);
```

Listing 2

```
begin
sasuser.PKG_AUTH_SAS_SESSION.sas_login(&_metaperson', '&clientuserid', '&sysuserid');
end;
```

Listing 3

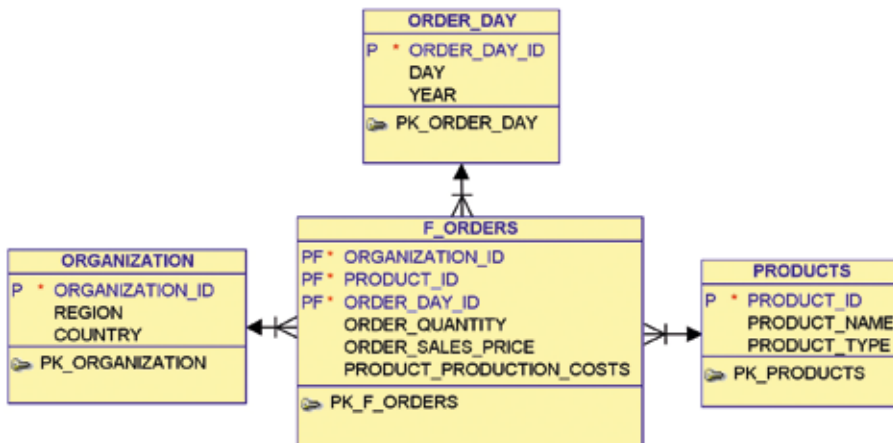


Abbildung 2: Beispiel für Stern-Schemata

REGION	COUNTRY
Europe	Switzerland
Europe	Austria
Americas	United States of America
Europe	Germany
Europe	United Kingdom
Europe	The Netherlands

REGION	COUNTRY
Europe	Switzerland
Europe	Austria
Europe	Germany
Europe	Others

Abbildung 3: Sichten auf Dimension „ORGANIZATION“

Oracle-Legitimation

Eine Anmeldung auf der Datenbank ist Voraussetzung für den Anwender-Zugriff. Sie geschieht typischerweise durch Angabe von Benutzernamen und Passwort. Zur Steuerung von Daten-Zugriffen verwendet man in der Regel Oracle-Rollen. Diese haben Zugriff auf Datenbank-Objekte. Mögliche Zugriffsrechte sind „Lesen“ (select), „Schreiben“ (update/delete/insert) oder „Ausführen von PL/SQL-Packages“ (execute). Die Datenbank-Anwender bekommen eine oder mehrere Rollen zugewiesen.

Für die Einschränkung von Daten-Inhalten existiert in Oracle-Datenbanken das Feature „Virtual Private Database“ (VPD). Es erlaubt die Beschränkung der Spalten-Inhalte und Datensätze. Zur Umsetzung wird eine Policy pro Tabelle definiert, die auf eine Policy-Funktion verweist. Diese wird bei jedem Zugriff ausgeführt und erzeugt zusätzliche Filter beziehungsweise blendet Spaltenwerte aus.

In unserem Beispiel führen zwei Anwender unabhängig voneinander die gleiche Abfrage aus (siehe Abbildung 6). Auf dieser Tabelle existiert eine VPD, die die Daten filtert. Beim Anwender „A“ wird durch VPD zusätzlich die Beschränkung auf „AT“ ergänzt. Im Ergebnis erhält der Anwender eine Zeile mit den entsprechenden Daten.

Anwender „B“ hat keinen Zugriff, angedeutet durch die Bedingung „1=2“. Dadurch ist die Ergebnismenge für ihn leer.

```
select REGION, COUNTRY, "USER" from sas_organization
```

REGION	COUNTRY	USER
Europe	Switzerland	Müller
Europe	Austria	Müller
Europe	Germany	Müller
Europe	Switzerland	Schmidt
Europe	Austria	Schmidt
Europe	Germany	Schmidt
Europe	Others	Müller

Abbildung 4: Spezielle Dimension „SAS_ORGANIZATION“ in Auswertungen

NIZATION“ erstellt (siehe Abbildung 4). Diese beinhaltet die individuellen Sichten auf die Struktur für jeden Anwender. Beim Befüllen der neuen Dimension mittels PL/SQL werden die Zuordnungen der SAS-Rollen je Anwender berücksichtigt.

Um sicherzustellen, dass beim Ausführen von Berichten und Analysen die korrekte Sicht verwendet wird, kommt Virtual Private Database (VPD) zum Einsatz. Allgemeine Informationen zur Legitimation in Oracle findet man im Infobereich. Zuerst wird die notwendige Policy auf dieser Tabelle definiert (siehe Listing 1).

Die zugehörige Policy-Funktion „F_AUTH_ORGANIZATION“ filtert für alle Anwender die Datensätze. Der technische User „SASUSER“, in dem die Tabelle liegt, erhält keine Beschränkung und sieht alle Datensätze. Für jeden weiteren User wird auf der Spalte „USER“ ein Filter angewendet.

In den Auswertungen der Anwender wird immer die „SAS_ORGANIZATION“ verwendet. Die Originaltabelle „ORGANIZATION“ wird für die ETL-Prozesse genutzt und dient als Basis für die „SAS_ORGANIZATION“. Einige Fakten-Tabellen und Berichte werden von mehreren Anwendern unterschiedlicher Themenbereiche verwendet. Allerdings sollen nicht alle enthaltenen Kennzahlen auswertbar sein. Im Beispiel enthält die Tabelle „F_ORDERS“ verschiedene Kennzahlen:

- ORDER QUANTITY
- ORDER SALES PRICE
- PRODUCT PRODUCTION COSTS

Sie wird von Anwendern der Themenbereiche „Sales“ und „Produktion“ verwendet. Allerdings soll „Product Production Costs“ ausschließlich für Anwender aus dem Themenbereich „Produktion“ sichtbar sein. Um die gesamten Daten zu sehen, müssen die Anwender Mitglied der SAS-Rolle „SAS PRODUCTION“ sein (siehe Abbildung 5). Die Umsetzung erfolgte ebenfalls durch VPD. Auf der Fakten-Tabelle wurde eine Policy definiert (siehe Listing 2).

Zur Definition der betroffenen Spalte werden zusätzlich die Parameter „sec_relevant_cols“ und „sec_relevant_

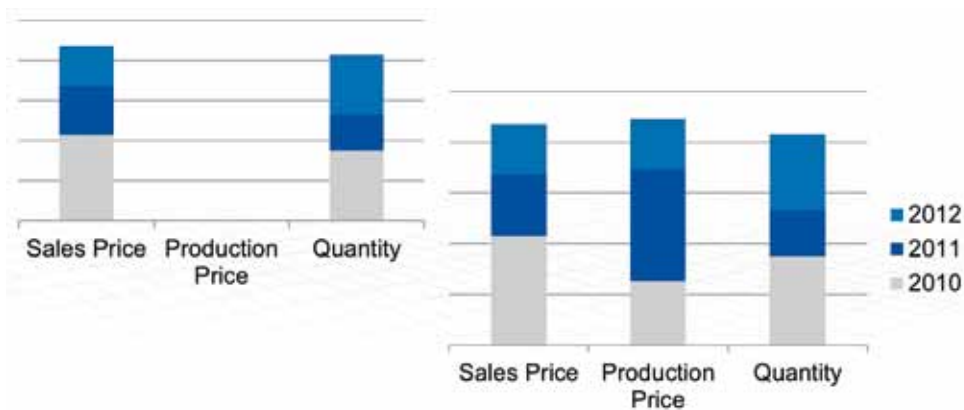


Abbildung 5: Darstellung beim Ausblenden von Kennzahlen in den Berichten für „Sales“ (links) und „Produktion“ (rechts)



Abbildung 6: Funktionsweise von VPD

Überblick SAS

Statistic Analysis System, besser bekannt als „SAS“, bietet verschiedene Komponenten für Daten-Bereitstellungen, Durchführung von Analysen sowie Definition von Berichten. Das SAS Information Delivery Portal kann im Browser dazu genutzt werden, Dashboards zu erstellen oder vorhandene Berichte zu öffnen. Zusätzlich kann das SAS Web Report Studio verwendet werden, um einfache Berichte zu erzeugen. Für komplexere Berichte dient die Windows-Anwendung Enterprise Guide. Basis der Berichte sind sogenannte „Information Maps“.

Sie werden im SAS Information Map Studio definiert (siehe Abbildung 7). „Information Maps“ sind Metadaten-Modelle und erlauben den Anwendern, einfach und ohne Kenntnisse der Datenbank-Struktur SQL-Datenabfragen durchzuführen. Die Möglichkeit einer Business-Sicht auf die Daten ermöglicht es, Informationen in Ordnern zu strukturieren, fachliche Bezeichnungen zu verwenden und Kennzahlen zu definieren.

Datenbank-Verbindungen werden in sogenannten „SAS Libraries“ definiert. Sie enthalten alle relevanten Informationen zum Erstellen der Verbindung. Dies ist vergleichbar mit der Definition einer Verbindung im SQL Developer. Die SAS-Daten (Information Maps, Berichte etc.) sind in den SAS-Metadaten abgespeichert – vergleichbar mit der Ablage von DDL-Informationen in einer Oracle-Datenbank.

Die Steuerung der Zugriffe auf die SAS-Metadaten erfolgt über Zuordnungen von SAS-Rollen und SAS-Gruppen. Der Anwender ist bei entsprechenden „Mitgliedschaften“ in der Lage, bestimmte SAS-Komponenten zu verwenden oder auf Objekte in den SAS-Metadaten zuzugreifen.

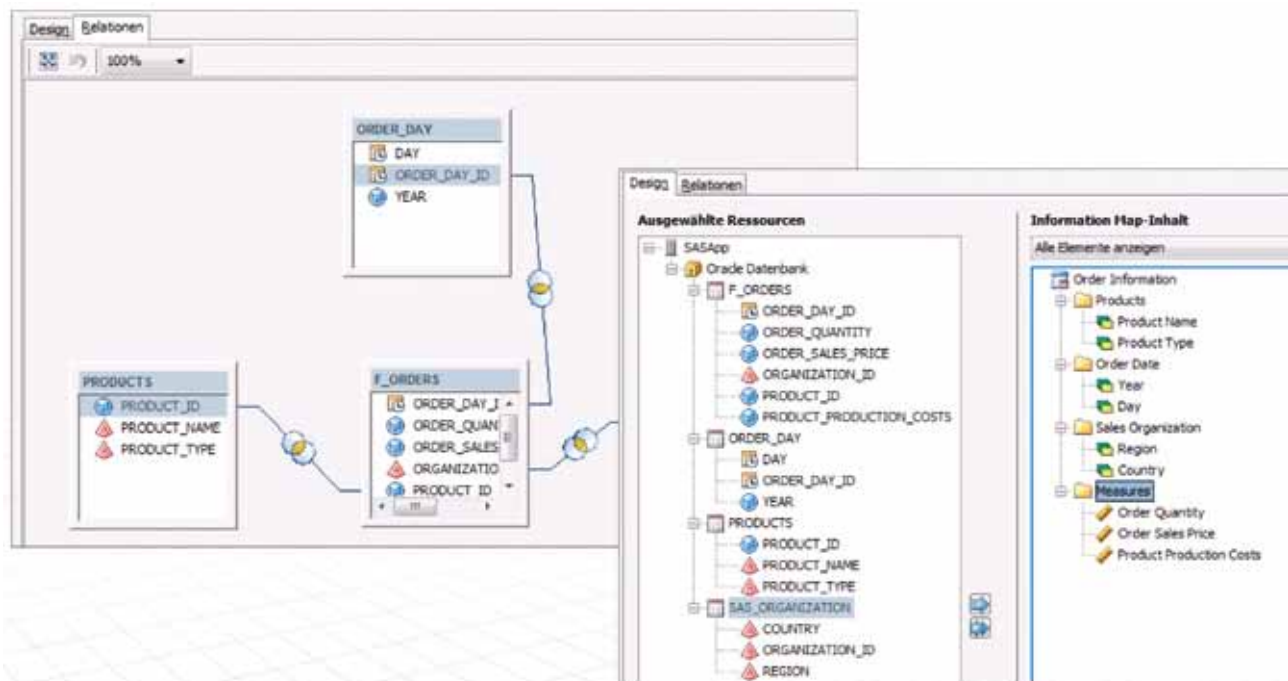


Abbildung 7: SAS Information Map Studio

cols_opt“ gesetzt. In der Policy-Funktion wird geprüft, ob der Anwender Mitglieder der SAS-Rolle „SAS PRODUCTION“ ist. Ist dies der Fall, wird der Inhalt der Spalte angezeigt – andernfalls wird „NULL“ ausgegeben.

Informationsübertragung zwischen SAS und Oracle

Zwei Punkte bleiben noch offen:

- Woher weiß Oracle, welchen SAS-Rollen ein Anwender in SAS zugeordnet wurde?
- Wie weiß Oracle, welcher Anwender in SAS angemeldet ist, wenn der Zugriff immer über einen technischen User erfolgt?

Jede Nacht werden die SAS-Rollen und Anwenderzuordnungen aus den SAS-

Metadaten in eine Oracle-Tabelle übertragen. Diese Informationen werden im Rahmen der Erstellung der Dimension „SAS_ORGANIZATION“ beziehungsweise in den Anwendungen der VPD berücksichtigt.

Die Anmeldung aus SAS an der Datenbank erfolgt immer mit dem technischen User. Für die Funktionen der VPD wird allerdings der korrekte Anwender aus SAS benötigt.

In SAS ist in unterschiedlichen Session-Variablen (je nach SAS-Komponente) der Benutzername gespeichert. Beim Aufbau der jeweiligen Datenbank-Verbindung werden eine PL/SQL-Prozedur aufgerufen und die Variablenwerte übergeben.

Oracle ermittelt den korrekten Anwender und hinterlegt ihn in einer Session-Variable. Die Policy-Funktionen

lesen die Session-Variable aus (siehe Listing 3).

Fazit

Unter Berücksichtigung der technischen Voraussetzungen und fachlichen Anforderungen konnte eine Lösung gefunden werden, die alle Bereiche erfolgreich abdeckte. Tiefgreifende Kenntnisse der eingesetzten Technologien von Oracle und SAS führten zur beschriebenen Realisierung. Die aufgezeigten Lösungen sind adaptierbar für zukünftig ähnlich gelagerte Anforderungen.

Christian Schütze
christian.schuetze@metafinanz.de

Impressum

Herausgeber:
DOAG Deutsche ORACLE-Anwendergruppe e.V.
Tempelhofer Weg 64, 12347 Berlin
Tel.: 0700 11 36 24 38
www.doag.org

Verlag:
DOAG Dienstleistungen GmbH
Fried Saacke, Geschäftsführer
info@doag-dienstleistungen.de

Chefredakteur (ViSDP):
Wolfgang Taschner, redaktion@doag.org

Redaktion:
Fried Saacke, Carmen Al-Youssef, Mylène Diacquenod, Dr. Dietmar Neugebauer, Stefan Kinnen, Dr. Frank Schönthaler, Christian Trieb

Titel, Gestaltung und Satz:
Claudia Wagner, Alexander Kermas
DOAG Dienstleistungen GmbH

Titelfoto: Fotolia

Anzeigen:
CrossMarketeam Doris Budwill
www.crossmarketeam.de
Mediadaten und Preise finden Sie unter:
www.doag.org/go/mediadaten

Druck:
Druckerei Rindt GmbH & Co. KG,
www.rindt-druck.de