Duty Segregation in the Oracle Database - Large Scale Rollout of Database Vault

Matthias Mann
Value Transformation Services S.r.l.
Munich, Germany

Keywords
segregation of duties, database vault, rollout procedure, realm, enablement tools

Introduction

In a database landscape based on RAC architecture and schema consolidated multipurpose databases legal requirements induced a large scale rollout and configuration of Oracle Database Vault (DBV). The configuration was kept as simple as possible by configuring application based realms. This was optionally combined with the use of Transparent Data Encryption (TDE). The presentation focuses on

- standardizing the rollout and configuration procedure
- description of the resulting duty segregation
- description of the necessary modifications for database maintenance utilities.

Database Cluster Architecture

The application services are bound to policy managed Real Application Cluster Databases on x86 based RedHat Enterprise Linux servers with usually two pools and 4 nodes per cluster (Fig. 1).

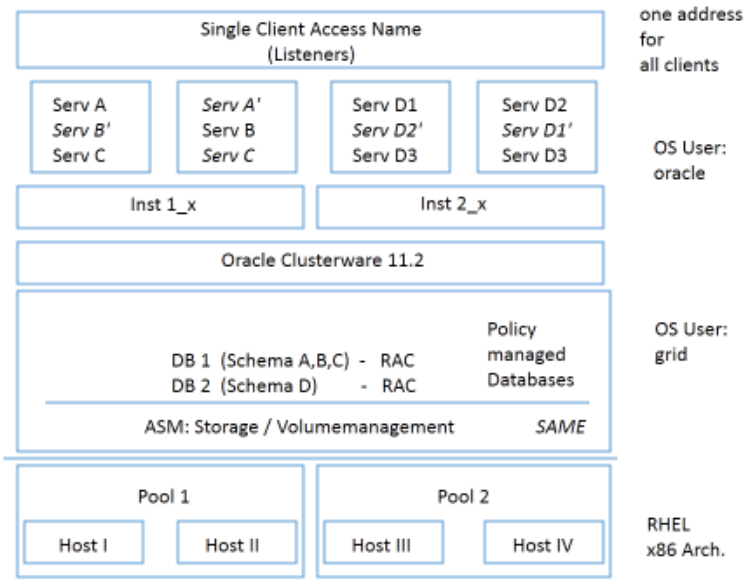

Fig. 1: Architecture of a standard application consolidated RAC

Legal Requirements and resulting Components of the Security Concept

Regulatory authorities for our client in the banking sector required the implementation of segregation of duties in accordance with MaRisk (Minimum Requirements for Risk Management, BaFin) on administrator level combined with an appropriate loggging.

This means, we needed to implement technical and organizational measures which guarantee:

- that DBAs cannot see or modify business data
- that DBAs cannot modify database user properties
- tracking of admin user activities

For Oracle databases a comprehensive security bundle consists of

- Database Vault
- Transparent Data Encryption
- customized database auditing.

Database Vault Basic Configuration

The DBV configuration in a schema consolidated multi application database was kept as simple as possible. To disable the DBA or other highly privileged accounts to see or modify business data each set of application schemas were protected by a database vault realm (see fig. 2). Customized proxy accounts enable application maintainers to manage the application schemas and data. For emergency situations a normally locked proxy account is available which can be used by the DBA group if needed.

Change of Administration Responsibilities

Due to enforced segregation of duties many resposibilities formerly executed typically by the DBA need now be done by other administrators as shown in table 1:

Category	**Restriction for DBA**	**in charge**
physical database backup	none	DBA
logical schema backup (datapump)	not possible	Appl. Admin
database statistics	none	DBA
index maintenance	possible with dedicated realm containing the indexes	Appl. Admin preferred
storage management	none	DBA
schema maintenance	not possible (only via emergency	Appl. Admin

	proxy)	
patching	possible with role dv_patch_admin (needs to be granted)	DBA, Security Admin
Upgrades	switch off DBV	DBA
account management	not possible	User Admin
DBV administration	not possible	Security Admin

Table 1: Duty Segregation in the vaulted database

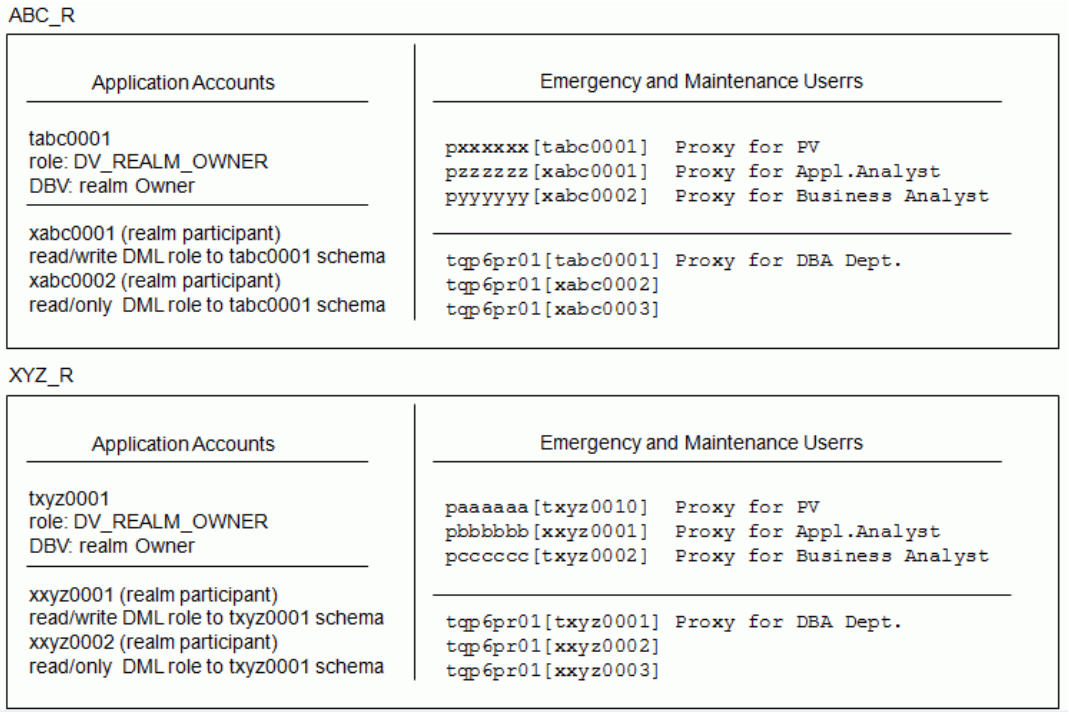

Fig. 2: Realms in a multiapplication database

Needed Processes and Workflows

It must not be underestimated that the enforcement of duty segregation requires a great deal of adaptation of existing processes and workflows. Examples are:

- management of functional database accounts
- granting permanent or ad hoc access to the database
- (privilege) management of personal databaase accounts

Along with this process adaptation training is needed for the various administrators to be able to manage their new duties.

Adaptation of Database Maintenance Tools

Many existing tools and scripts previously used only in the DBA group had to be adapted to the segregation of privileges in the database. We mention here scripts for granting and refreshing privileges and datapump tools. The main changes to implement were:

- make the tools client / server capable
- make the tools executable by a schema owner instead of the DBA
- take into account DBV peculiarites.

Standardization of DBV Rollout Procedures

The configuration of DBV in a general purpose database, which is historically grown, is a complicated process which requires a lot of considerations. Before the rollout we developed a standardized approach to assess the existing privileges in a database and make the configuration DBV compatible. Topics of special attention were

- database roles and their management
- public synonyms and privileges.

The "conversion" to a DBV compatible configuration was done by executing the following steps:

- check / activate software and database options
- make an inventory of all existing privileges
- enable database vault in the database
- clean up existing admins, configure named DBAs and User Admins
- create procedures for schema management
- investigate about public synonyms and privileges
- create and configure realms
- disable role management
- protect audit trail

Contact

Dr. Matthias Mann
Value Transformation Services S.r.l.
Am Tucherpark 12
80538 Munich
Germany

Telefon: +49 89 378 20314
E-Mail matthias.mann@v-tservices.unicredit.de