Comprehensive database security - can it be achieved even with a SE2?

Mag. Dr. Thomas Petrik
Sphinx IT Consulting
Wien

Keywords

Oracle Database, SE2, Security, Standard Edition, VPD, TDE, Encryption, RLS

Introduction

Enterprise Edition users have a complete portfolio of security features at their disposal either as part of EE itself or as part of the Advanced Security Option. Standard Edition users, however, do not even have the possibility to buy an extra option. Nevertheless, many of these security features can be implemented using available Oracle standard tools and OS methods. There are also some third party tools available which are not restricted to a specific edition.

Row Level Security

In EE the Virtual Private Database (VPD) is used to implement row level security (RLS). In a Standard Edition RLS can be implemented in a View layer with different methods:

a) Functions
b) Application context (global or local)
c) Joins with access configuration tables

Functions may be deterministic or not and a context can be used with dynamic caching or as a static context.

These methods differ in performance and usability depending on the targeted security scenario as well as on the size of the datasets and the structure of the queries. Benchmarks will show the differences in detail, especially in relation to an implementation of a VPD.

Tablespace encryption

Especially in an outsourcing scenario where the hypervisor admin is an external resource it is a big risk to use unencrypted storage in the virtual environment. The lecture will demonstrate how easy it is to access any data from the hypervisor layer and what methods can be used in order to mitigate this risk even if Transparent Data Encryption (TDE) is not an option. Benchmarks will show the possible performance impact of the methods chosen.

Backup Encryption

Backup security has basically 2 components: the security of the transfer method and the security of the backup set at the destination. Without RMAN encryption (which is also part of the Advanced Security Option) an encrypted transfer protocol must be chosen and the backup set at the destination has to be encrypted itself or must follow similar rules as the tablespace encryption. Besides, a possible space reduction should be considered by using compression or deduplication techniques.

Access Control

In the absence of DB Vault a logon trigger based security framework seems to be the best solution. However, several restrictions apply and it is impossible to achieve separation of duties. The lecture will explain advantages and limits of such a technique and some use cases for database firewalls from third party vendors will be discussed.

Fine grained DDL and DML Control

Sometimes it is necessary to restrict even the owner of an object to modify it (both, with DDL or DML). While DB Vault is used for this purpose in EE one can implement a trigger based solution in SE2 in order to achieve nearly the same result. Pits ad falls as well as limits of this method will be discussed.

Conclusion

While audit and client/server encryption are available in SE2 in the same way as in EE the features of VPD, DB Vault, TDE and backup encryption can be replaced in a Standard Edition to an impressively high extent mainly by using Oracle standard techniques and some OS features. Some limits like separation of duty for the DBA can be overcome by the introduction of third party tools like database firewalls or external filesystem encryption tools.

Contact:

Mag. Dr. Thomas Petrik

Sphinx IT Consulting

Aspernbrückengasse 2

A-1020 Wien

Phone:	+43 664 155 8304
Fax:	+43 (1) 599 31-99
E-Mail	Thomas.Petrik@sphinx.at
Internet:	www.sphinx.at