# Audit report on database security and performance management

Technology, Computer

EXECUTIVE SUMMARY

This report covers a review of the Security and performance issues, with the respect to the size and capacity of the data management in Organic Cosmetics Ltd. We are running a company with a total number of over 100 employees and large customer base national and international.

In summary, we found some deficiencies in security integrity and performance in terms of query optimisation and as well as areas where improvements are warranted as listed below;

1. No proper procedure of reducing Sensitive Data Exposure which will in turn be devastating to the company, if not sorted out as soon as possible.

2. Deficiency in the way of detecting Threats from Inside and Outside

3. Deficiency in the way of developing Secure Applications

4. In terms of performance optimisation, there is no proper indexes set up to optimise and speed up retrievals of queries that are taking too long to execute.

AIMS AND OBJECTIVES

The main aim for the report is to carry out the proper procedures and techniques that is best to carry out the better security performance and query optimisation for administrative management performance. And after a proper consultation with experts and detailed research we have all that is takes to implement and effect changes to these deficiencies.

Some of our objectives are; Reducing Sensitive Data Exposure in Applications by introducing an Oracle Advanced Security data redaction which provides selective, on-the-fly redaction of sensitive data in query results prior to display by applications.

Limiting Sensitive Data Exposure When Sharing Data, we have been able to put in place Oracle Data Masking and Subsetting.

Deficiency in the way of developing Secure Applications, we have been able to source out advanced and more sophisticated security measures introduced by oracle Database 12c Real Application Security, which is Oracle’s next generation database authorization framework and the industry’s most advanced solution for developing secure applications called Basic Fine Grained Access Control (Oracle Virtual Private Database (VPD)) and the Real Application Security (RAS).

Performance optimisation, there is no proper indexes set up to optimise and speed up retrievals of queries that are taking too long to execute. There should advance form of scalability which is the ability of a system to process more workload, with a proportional increase in system resource usage, there we have to choose an efficient execution strategy for processing a query.

APPROACH

The best possible way of reducing sensitive date exposure is by the Redaction process. Redaction is the process of scrubbing out data. Imagine a paper document with certain fields scratched out with a black marker. Oracle

Advanced Security data redaction works similarly but on application data stored in the database. Because it is enforced inside the database, it is possible to consistently redact database columns across different application modules accessing the same data. Data redaction minimizes changes to applications because it does not alter actual data in internal database buffers, caches, or storage, and it preserves the original data type and formatting when transformed data is returned to the application. Data redaction has no impact on database operational activities such as backup and restore, upgrade and patch, and high availability clusters.

Because we handle a lot of big transactions OCL, it will be better to use data redaction to make sure our data are secured.

The movement of production data dramatically increases the risk to data and increases the overall cost of security and compliance. Masking of data before it is moved from production eliminates the risk of data breaches in non-production environments by irreversibly replacing the original sensitive data with fictitious data so that data can be safely shared.

Using Oracle Data Masking and Subsetting enables entire copies or subsets of application data to be extracted from the database, obfuscated, and shared with partners inside and outside of the business. Most importantly, during the obfuscation process, application integrity is preserved by maintaining data relationships across application tables. Oracle Data Masking and Subsetting improves security by reducing the scope of data

exposed to partner organizations. Compliance costs are lowered by narrowing the compliance boundary for test and development groups.

Below is an example of data being masked. Instead of four rows in Name and salary column the masking has reduced it the rows and interchanged the data store in each column rows.

The solution to deficiency in the way of developing Secure Applications is by adopting the following process, which we have been able to source out. It is an advanced and more sophisticated security measures introduced by oracle Database 12c Real Application Security, which is Oracle’s next generation database authorization framework and the industry’s most advanced solution for developing secure applications called Basic Fine Grained Access Control (Oracle Virtual Private Database (VPD)) and the Real Application Security(RAS).

Oracle Virtual Private Database (VPD), introduced in Oracle8i, is widely used today to enforce fine grained access control within applications. It allows application developers to associate a stored PL/SQL program unit with an application table, view, or synonym. The program unit fires when the application object is accessed via SQL. The program unit computes a predicate or ‘ where clause’ that is appended to the original SQL statement. In many cases, the program module will query specific meta data tables containing information on user roles and privileges as nearly every application today has its own unique set of security tables. Another common

approach used with VPD is to initialize an Oracle application context when a new application user is initialized within the application.

Real Application Security(RAS).

Unlike the basic Oracle Virtual Private Database (VPD), Oracle Database 12c Real Application Security (RAS) provides a robust declarative model that allows developers to define the data security policy based on application users, roles and privileges within the Oracle Database. The new Oracle Database 12c RAS technology is more secure, scalable, and cost effective than the traditional Oracle VPD technology.

Real application security provides a declarative interface that allows developers to define the data security policy, application roles, and application users without requiring application developers to create and maintain PL/SQLstored procedures. The data security policies are defined inside the database kernel using the Oracle Database 12c RAS API. The permissions associated with business objects are stored in Access Control Lists (ACLs).

ACLs are a key component of RAS and store the privileges assigned to principals and control the type of operations: select, insert, update and delete that can be performed on the objects.

These are some of the usefulness of Real Application Security provides the next generation authorization architecture for applications that will be needed in Organic Cosmetics Limited (OCL):

1. Uniform Data Security: The RAS Security model allows uniform specification and enforcement of access control policies on business objects irrespective of the access path. It overcomes the limitation of custom built approaches that only work when an object is accessed via the specific code path that has access control logic embedded into it.

2. Secure End User Identity Propagation: Application sessions allow the end user identity and associated attributes to be conveyed securely to the database allowing the database to use the information for end-user access control and auditing.

3. Declarative and Fine Grained Access Control: RAS policy components encapsulate the access control requirements of the application in the form of declarative policy on data for application users, application roles, and application privileges. With column security, RAS model extends authorization to the column level to protect sensitive data such as SSN. With support for master-detail, parameterized, delegation, and exception based declarative policies, RAS meets the real-life deployment requirements of applications.

Then for the issuesof performance optimisation and quick table accessibility, there is no proper indexes set up to optimise and speed up retrievals of queries that are taking too long to execute. Finally, there is an indexing system that can be set up to help sort the out accessibility of records quickly. Basically there are 3 kinds of index, but we have chosen the

Function index. In a function index you index an expression rather than a column.

Eg supposing you wanted to regularly retrieve orders that haven’t been shipped, so no value in ‘ shipdate’. A basic B-tree index couldn’t be set up because it wouldn’t include nulls in the index, so function based could be used:

eg:

CREATE INDEX non_shipped_index

ON ordA (NVL(shipdate, ‘ null’));

CONCLUSION AND RECOMMENDATION

Based on our findings and recommendations I believe if we could make appreciate changes as soon as possible we can be able to sort the deficiency issues in our database management system and also to improve our services.

1. 4 REFERENCES

WHITEPAPER, O. (2015) Oracle Database 12c Security and Compliance. Available at: http://www. oracle. com/technetwork/database/security/security-compliance-wp-12c-1896112. pdf (Accessed: 08 February 2017).