Managing access to enterprise information based on the mandatory model

IOP Conf. Series: Materials Science and Engineering **483** (2019) 012022 doi:10.1088/1757-899X/483/1/012022

Managing access to enterprise information based on the mandatory model

A S Ksenofontov, I I Mamuchiev, L A Moskalenko

Federal State Budgetary Educational Institution of Higher Education «Kabardino-Balkarian State University named after H.M. Berbekov», 173 Chernyshevsky Street, Nalchik, 360004, Russia

E-mail: misteribragim@yandex.ru

Abstract. The article describes the main aspects of working with Oracle Label Security (OLS), discusses the OLS capabilities for managing access to corporate data. The access to information is controlled by the OLS policy, which has a standard set of components: Labels, Levels, Compartments (optional security levels), Groups (optional security levels), Policy. The proposed methodology complies with the requirements of the Government of the Russian Federation "Digital Economy of the Russian Federation" program among the main end-to-end digital technologies, which include big data.

1. Introduction

The purpose of the work is to study the main aspects of the work of Oracle Label Security and apply the use of data labels to limit access to enterprise information using OLS.

For the past 30 years, Oracle has been a leader in developing advanced data protection solutions that enable the security of sensitive information. Oracle Label Security (OLS) is part of Oracle's in-depth approach to security and is considered the most advanced information access control solution based on information classification. This ability is crucial to ensuring the "need-to-know" principle for accessing data and combining information. Combining information not only reduces the cost, but also increases the efficiency of analysis and the effectiveness of decision-making [1].

The need for the most sophisticated means of controlling access to sensitive information is becoming increasingly important as companies address emerging security requirements with regard to data fusion and confidentiality. In particular, maintaining separate databases (DB) for highly sensitive customer data is costly and incurs unnecessary administrative costs. OLS guarantees the ability to label information with a data label or a classification of information. This feature allows the database to know, in essence, what information is sensitive, and allows sharing secret information in the same table as the entire data set, without compromising security (Figure 1).

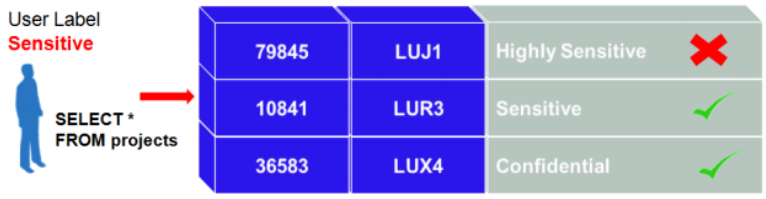

Figure 1. Access Control OLS.

2. Access to secret data

Access to sensitive information is controlled by matching the data label with the requesting user or security label. A custom label or security permission can be viewed as an extension of standard privileges and database roles. OLS is used in the database under the application level, providing reliable protection and eliminating the need for complex application representations [2].

The classification of information plays a vital role not only in adhering to the need-to-know principle, but also in reliably combining highly sensitive information. Historically very sensitive information is stored in physically separate systems. But this approach has limited the ability to perform advanced analysis and business intelligence. OLS provides the most advanced and flexible solutions for classifying information [3].

OLS applies information at the row level to provide access control that restricts users to information that they are allowed to access. This allows organizations to control their own operating and storage costs, allowing information with different degrees of sensitivity to be combined in the same database [4].

A characteristic feature of the OLS function is the multi-level access policies that allow you to store access control attributes in clusters.

Inside the policy, data access levels are defined: “highly sensitive”, “sensitive” and “confidential” information or other sets of levels: “top secret”, “secret”, “confidential” and “unclassified”. In addition to these levels, there are four more: “trade secret”, “proprietary”, “company confidential confidentiality” and “public domain” [5]. A user with a higher level of access has access to information marked with its level and levels below.

OLS is a commercial option for Oracle Database Enterprise Edition [6].

The OLS policy has a standard set of components:

– Labels. Labels for data and users, as well as permissions for users and software units, regulate access to marked protected objects. Labels consist of the following elements:

– Levels. Levels indicate the type of sensitivity you wish to assign to a line, for example, sensitive or highly sensitive.

Optional security levels:

– Compartments. Information may have the same level (public, confidential and secret), but may belong to different projects within the company, for example, ACME Merger and IT Security. Departments present projects in this example that help establish more accurate access controls. They are most often used in public institutions.

– Groups. Groups establish companies that possess or acquire access to information, for example, in the UK, USA, Asia, and Europe. Groups are used in both commercial and state environments and are often used instead of departments because of their flexibility.

– Policy. Policy - the name associated with labels, rules, authorizations and protected tables [7].

3. Mandate access model

Mandatory access control (mandatory access control, MAC, sometimes translated as compulsory access control) - delimiting the access of subjects to objects, based on the assignment of a confidentiality label for information contained in objects, and issuing official permits (access) to subjects to access information of this level confidentiality.

According to the requirements of the FSTEC, mandatory access control or “access labels” are considered to be the key difference between the protection systems of the State Secrets of the Russian Federation of the senior classes 1B and 1B from the junior classes of the protection systems on the classical division of rights in the access matrix.

The main purpose of the BCH is to prevent information leaks from objects with a high level of access to objects with a low level of access.

For systems with the BCH, the security check task is algorithmically solvable. Such systems are characterized by higher reliability. The disadvantage of the BCH is a higher complexity of implementation [8].

There are requirements for a mandatory mechanism, which are as follows:

1. Each subject and object of access must be associated with classification labels reflecting their place in the corresponding hierarchy. Subjects and objects should be assigned classification levels using these labels. These labels should form the basis of the mandatory principle of access control.

2. The security system when entering new information into the system should require and receive from the authorized user the classification labels of this information. When authorized to add a new subject to the list of users, a classification mark must be assigned to it. External classification labels (subjects, objects) must exactly correspond to internal labels (inside the protection system).

3. The protection system should implement the mandatory principle of access control for all objects with explicit and implicit access from any of the subjects:

a) a subject can read an object only if the hierarchical classification in the classification level of the subject is not less than the hierarchical classification in the classification level of the object (Figure 2).

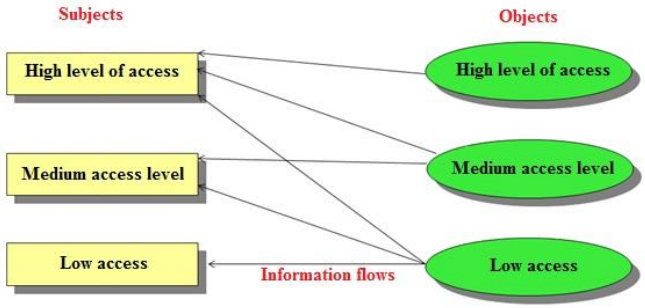

Figure 2. Reading information.

b) the subject realizes writing to the object only if the classification level of the subject in the hierarchical classification is not greater than the classification level of the object in the hierarchical classification (Figure 3) [9].

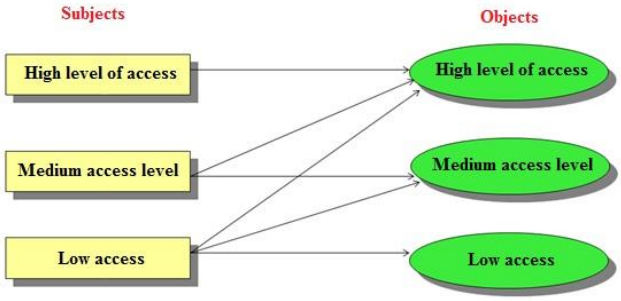

Figure 3. Recording information.

There is also a place to consider the Bella LaPadula model - one of the first security models - and subsequently the most frequently used one. The model was developed by David Bell and Leonardo LaPadula to simulate computer operation. To illustrate the model, consider a system of two files and two processes (Figure 4). One file and one process are unclassified, the other file and process are secret.

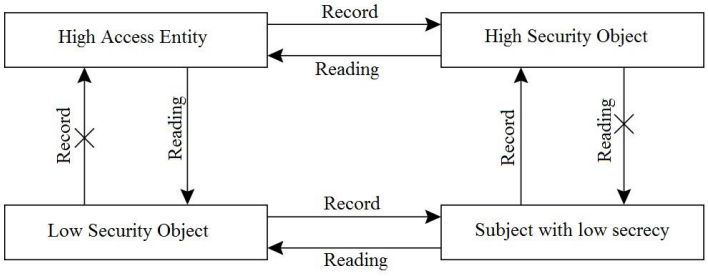

Figure 4. Illustration of the Bella LaPadula model.

The implementation of the mandatory rules of access control should take into account the possibility of tracking, changing the classification levels of subjects and objects by specially selected subjects.

Advantages:

– With the help of multi-level models, a significant simplification of the administration task is permissible. Moreover, this applies both to the initial setting of the demarcation access policy (such a high level of detail in the setting of subject-object relationship is not required), and to further incorporation into the administration scheme of new objects and access subjects.

– The most important advantage is that the user cannot fully control access to the resources that he forms.

– Such a system prohibits a user or process with a certain level of trust from gaining access to information, processes or devices of a more protected level.

Disadvantages:

Separately taken categories of the same level are equivalent, which in most cases leads to redundancy of access rights for certain subjects within the limits of the corresponding levels [9].

4. Differentiation of access to database resources

We describe for each group of users the rights of access to each table. Access rights must be distributed so that for each database object there is at least one user who has the right to add and delete data from the object. The rights are shown in table 1.

Table 1. Access rights to database resources for user groups

Tables	User groups (roles)						
	A	B	C	D	E	F	G
Employee	SIUD	SIUD	S	SIU	SIUD	-	S
Department	SIUD	SIUD	S	SIU	SIUD	-	S
Location	SIUD	SIUD	S	SIU	SIUD	-	S
Job	SIUD	SIUD	S	SIU	SIUD	-	S
Customer	SIUD	SIUD	-	-	-	-	S
Sales_order	SIUD	SIUD	-	-	-	-	S
Item	SIUD	SIUD	-	-	-	-	S
Product	SIUD	SIUD	S	S	S	S	S
Price	SIUD	SIUD	S	S	S	S	S

Where: S - data reading (select); I - add data (insert); U - data modification (update); D - delete data (delete), A - Database_administrator, B - Director, C - Employees, D - Bookkeeping, E - Human_Resources_Department, F - Client, G - Special_privileges.

Rights are assigned by the DBA (or security administrator, if the system is complex and there are several administrators).

Practical implementation of mandatory access control to data by means of Oracle Label Security: 1) creation of users; 2) giving users the right to create a session with the server; 3) provision of administrator rights and the right to create tables and unlimited table space; 4) the creation of tables; 5) establishing links between relational database tables; 6) filling in tables with data; 7) creating OLS policies; 8) adding labels on lines; 9) change of policy on enforcement during reading; 10) the issuance of the right to read the protected OLS table without any specific level of tolerance; 11) view table entries through users.

5. Conclusions

As part of this work, the following tasks were performed: 1) analysis of the subject area, database design at the logical level; 2) implemented a database in the environment of Oracle Database Enterprise Edition; 3) selected user groups, their functions, tasks and requests; 4) accounts of user

groups are created and administered on the basis of the mandatory access model; 5) information is marked with a data label or information classification; 6) the mandatory access restriction model has been adapted for individual records of the table; 7) an algorithm has been developed for differentiating access according to the mandate model; 8) secured security policy in multi-user database systems; 9) access control to database resources has been implemented by means of the OLS function; 10) formed a database security administrator's guide.

The server database contains 9 tables with the following number of records:

Employee table - 32 entries. Department table - 11 entries. Location table - 4 entries. Job table - 6 entries. Customer table - 33 records. Table Sales_Order - 100 records. Table Item - 271 entries. Product table - 31 entries. Price table - 58 records.

Selected 7 groups of users and transferred to the platform Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production, each filled with 7 accounts.

The accounts are object and operator-administered on the basis of the mandatory model.

A database security administrator's guide has been developed, which describes how to install and configure the operation mode in Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production and activate the Oracle Label Security feature.

Testing of user groups access to database resources was carried out using a specific example.

When using the mandatory access restriction model, the BOP is fully controlled by the server security administrator.

The proposed methodology meets the requirements of the Government of the Russian Federation "Digital Economy of the Russian Federation" program among the main end-to-end digital technologies, which include big data.

References

[1] Oracle Label Security. Technical White Paper. ORACLE WHITE PAPER | MARCH 2018 [Electronic resource] Access mode: http://www.oracle.com/technetwork/wp-dbsec-ols-201702-3634252.pdf

[2] An Oracle White Paper June 2013. Oracle Label Security with Oracle Database 12c [Electronic resource] Access mode: http://www.oracle.com/technetwork/database/options/label-security/label-security-wp-12c-1896140.pdf

[3] An Oracle White Paper March 2009. Oracle Label Security in Government and Defense Environments [Electronic resource] Access mode: http://www.oracle.com/us/products/database/database-govdef-label-security-twp-066569.pdf

[4] Oracle Label Security 18c [Electronic resource] Access mode: http://www.oracle.com/technetwork/database/options/label-security/index-084797.html

[5] Oracle Database Release 12.2. Administrator's Guide. 2 Understanding Data Labels and User Labels [Electronic resource] Access mode: https://docs.oracle.com/en/database/oracle/oracle-database/12.2/olsag/understanding-data-labels-and-user-labels.html#GUID-2C0383D3-4AA5-4263-B938-827E2CCC40C0

[6] Oracle Label Security. First acquaintance [Electronic resource]. - Access mode: https://habr.com/post/185946/

[7] Oracle Label Security. Administrator's Guide 12c Release 2 (12.2). May 2017 [Electronic resource] Access mode: https://docs.oracle.com/en/database/oracle/oracle-database/12.2/olsag/introduction-to-oracle-label-security.html#GUID-ACEE3C58-A7CF-4548-976C-7D1C9F79A047

[8] Security database systems. 2. Access control [Electronic resource] Access mode: https://ppt-online.org/68872

[9] Access control models: discrete, mandatory, role [Electronic resource] Access mode: http://gman1990.ru/articles.php?article_id=83