ATLANTIS PRESS
Advances in Engineering Research (AER), volume 82
2016 International Conference on Engineering and Advanced Technology (ICEAT-16)

Study on a New Type of Database Security Audit System Based on Confidentiality

Ye HUA, Yuan-Yuan MA and Xiu-Li HUANG
GLOBAL ENERGY INTERCONNECTION RESEARCH INSTITUTE

KEYWORDS: Confidentiality;Database security audit system;Data module;Audit model

ABSTRACT: With the rise of the database's capacity, the pressure of the audit security system has also increased dramatically. Therefore, in view of the current mainstream of the database audit system operation mechanism, the author work on finding the cause of inefficiency of audit mode, uneven distribution and the poor confidentiality. And the paper through analysis comprehensively and understands the data distribution and statistical rules under the framework of the system, designing a new database security audit system based on confidentiality.

INTRODUCTION

Potential security risks of the current variety of database systems are mostly derived from the system's internal attacks, while the ability of existing database retrieval system against for internal attacks is very limited. In addition, with its own nature of variability and the concealment the external attacks to database , the existing defensing Intrusion Detection System(IDS) is difficult to make the deal quickly and effectively. However, the current mainstream database security audit system has not open up specifically an independent audit interface, which needs operators start-up manually the audit function and finish manual configuration leading to review work being more heavy and the lack of efficiency. Therefore, the field of audit need a type of general audit system, which has the ability of solving perfectly the different database system's version requirements, and replacing the manual configuration, simplifying the process, and improving stability and confidentiality of database systems.

1 Analysis on mainstream database audit module

The current widely used database systems are more mature with higher performance ,such as Oracle Microsoft SQL server, IBM DB2 and so on. And above database systems' audit modules include: standard information collection base with four sub - diversity,including: the set of main body, the set of object, the set of rights, the set of statements. What's more, the four types of sets form a common core audit control switch determining the exercise conditions for functions in order to count in the specific data audit records that named AUDS table after further screening.

Other types of database and the exercise of functions are similar with the above database's structure. And in the table of SYS.ADUS, the system will organize and create some pieces of parallel system views independently for users managing and querying the records of audit process. However, even the mainstream database configuration still has phenomena,such as redundancy of audit information and waste of physical space.

Investigating its fundamental, it is can be concluded that the lack of unified audit system is the core of these phenomena lies in the process of database audit system framework,so it needs to formulate standardized audit rules and information recording format. At the same time, in the

process of exchanging database's information product, if it is lack of a visual query interface with convenient configuration, then subsequent database collation will be more tedious, and the maintenance for DBA audit will be more troubled, which means that it will influence the efficiency of database audit. Therefore, confused date interfaces also greatly reduce the confidentiality and security of database's information.

2 New type of database security audit system

Based on all kinds of problems existing in the database system, because the security is not guaranteed, so it needs to overthrow the imperfect design and finish the redesign to achieve the functions of new type of database security audit system.

2.1 Framework of new type of audit system

In order to achieve the security level of the standard requirements, and ensure the stability and security of the database, it is needed to add some new audit system modules on the previous mainstream database configuration system. As shown by the table below, on the basis of the original audit system making some change including four new modules and two built-in data pools which named "Information audit process recording module","Privilege audit query rules module","Information distributing query module","Statistical analysis report module","Audit's rule of authority management library" and "Classification Library of statistical rules and features".

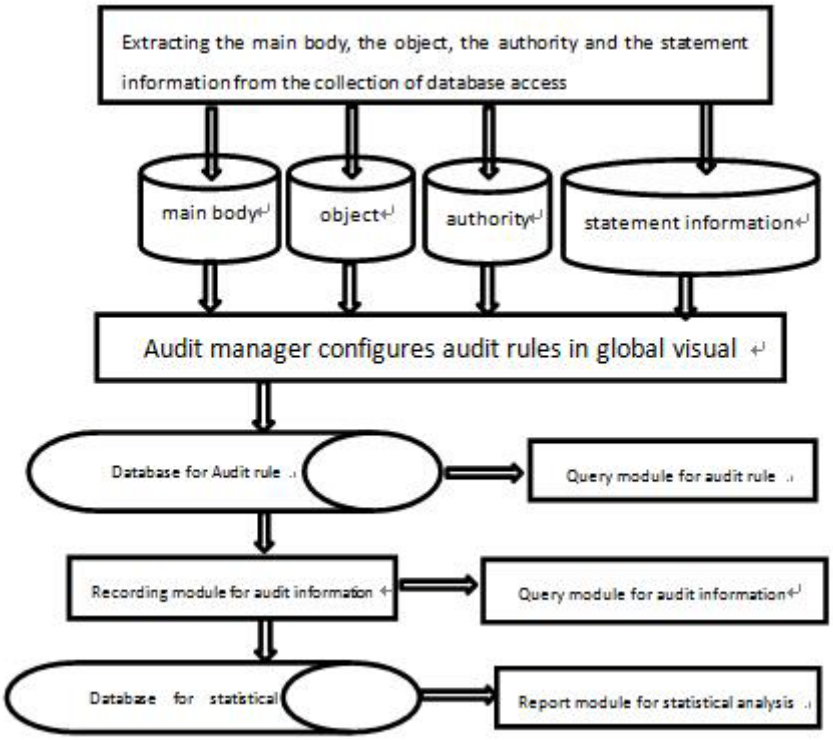

Figure 1 Mainstream database audit module

For coordinating the function and configuration of the relationship between configuration modules, firstly, the administrator of the audit shall, according to the requirements of the database management, and level of security and confidentiality of information, finish the work about corresponding configuration audit rule management library and divide the rights and information

retrieval extraction channel in detail, what's more, according to different requirements for channel's safety, generating detailed record information. At the same time, the creation of a special audit query management module for the administrator to check changes regularly which can not only improve the confidentiality of database, but also strengthen the tightness of management for the database tight.

2.2 The establishment of audit configuration for rules library

Based on the content of database, and if the read and write in a single time of the system become more frequently, then each operation completed is in accordance with the process of recording, and the record memory will be increased in double. Following the general rules of the audit framework to develop and to enhance the appropriate security measures and level of database's security audit rules,it can be concluded as that the key information of the audit is more pertinent, which is conducive to the retrieval and removal of the threat lying in database's security. And to a certain extent, formulating general rules and framework for audit work and simplify the operation scale and reduce the waste of memory.

The following gives a detailed definition of the rules database:

(1)Security Auditing Rule: Security Auditing Rule is a group including seven elements which means SAR=(AO, OP, T, M, SL, AF, S):

AO=(Pr, Sa, U, O) specifically refers to the main object of the audit, can be divided into, Pr={pr1, pr2, pr3,... } which specifically refers to the collection for the rule of privilege in scope of audit rules that needs to conduct a unified name. And Sa={sa1, sa2,sa3,... } which refers to the set of statements that need to be audited in the audit language module. U={u1, u2, u3,... } which refers to in the process of the user auditing information, the collection of permissions related to the name of objects. O={o1, o2, o3,... }, which means establishing consistent set in the information database approved by audit objects.

OP=(op1, op2, op3, …)means symbol set for all related operations and data changes on the audit subject.

T={t1, t2, t3, …}refers to the collection of all different audit categories in which the value of T (1,2,3,4) stands for privilege audit, statement audit, user audit and object audit.

M={m1, m2, m3, …}is a collection of all audit models that are used to record the success and failure of audit and the operation of related audit changes.

SL means the security level of audit rules which is roughly divided into low, middle and high. According to the actual database and work experience, audit manager divides subject to be audited into different levels of security.

AF refers to the frequency of audit which belongs to basic operation set including three parts: the frequency of conversation, the frequency of visits and the frequency of transactions.

S is used to realize the switch function of the audit with a set of symbols to control the opening of a new audit rules or divide the new data inventory, and vice versa.

All of the above functions are based on the running rules formulated by administrator which is a limited set. Therefore, each of the audit rules must have a specific operation event of database to be corresponded, and then in accordance with the the relationship between audit configurations to finish work of audit.

2.3 Instance test for security rule audit

sar1=(sys.aud S, drop, 4, a, high, access, true)

According to the above audit rules,it can be drawn that the code "sys.aud S"refers to start-up the

highest level of security of audit strategy database, if there is “drop” related operations in the next process, then it can be regardless of the execution results which means it will continue to visit frequency of audit whether it is success or not.

Among them, which is worthy of attention is that when the object of data audit or updated user was altered, and at this time, it may have lead to errors in audit rules causing the dislocation of the audit database. For example, when removed a piece of obsolete form,then the audit rules in the form become invalid, and it means the audit manager need to delete it in time, otherwise if the database operation related to the audit rules but couldn't find the source data, the procedures will report errors, and it will affect the running of audit rules.

In addition, in the different types of audit information, the object of the symbol and the meaning of operation are different. Therefore, in order to facilitate the administrator to query and sort out the existing audit rules, it needs to set up privileged audit, statement audit, customer audit, object audit under the audit system, and these four parts belong to data rule base.

In short, based on the above cases, in the process of audit, it should try to avoid unnecessary overflow of information, while screening for enough effective information to be handled and stored the data into the database. In addition, the administrator needs dynamic monitoring, and develop a reasonable audit unit security data system to avoid the threat of wrong estimates and hidden dangers.

3 Audit format and adaptive model

3.1 Uniform standard for audit format

There are two ways to upgrade the information record format for database which are Bishop standard of location and tracking in audit format and the format of normalized data method. For bishop tracking scheme, every log system contains different domains, and each different domains use the symbol “#” to be divided, and with the start symbol “s” and termination symbol “e” to determine the scope and size. The contents of the domain are all composed of code ASICII. What’s more, the reason for choosing code ASICII is that it can effectively avoid the problem of overflowing data and compatibility of format which may exist in floating point data. In the normalization of the audit method, it is that each key design data exists in the NADF records which are developed independently. And each record contains three characteristics which refers to identification mark of the data, the audit data type, the length of the numerical measurement.

Now, based on requirements of confidentiality, and with the original normalized rules, it can expand a new NADF data format, in that the each information record can contain up to 11 characteristic domains, or there are at least 6-7 feature domains to determine the only main body of operation,the object and the specific contents of data operation. And record format definition is given below:

(Security Auditing Trail Format)

SATF =(U, UID, O, OID, T, SQL_TEXT, TIME, IS_SUC, ERR, Hostname, IP)

In the format, the main body of the information records, the main identifier, the object and the object identifier respectively referred by U, UID, O and OID. Post sequence symbols means the specific operation of the SQL statement or the TIME of operation, as well as the results after the operation to determine whether the operation is effective. And if the operation fails, the error record information is displayed, otherwise the output will be empty.

3.2 Build adaptive model

3.2.1Selection of characteristic value

The model of audit analysis is mainly based on the historical archives, which is used to judge whether the subjects of events deviate from the original mode of action. Setting the statistical threshold value to calculate the deviation degree of information in each audit.

The specific abnormal characteristic value should be based on the characteristic value influencing choice of factors in the unusual invasion behavior. And according to the existence of the intrusion mode in database, it can be subdivided into the strength class and entity class. Features of entity attack are mainly focused on tamper of objects for users and the access to steal or replace by users. While the intensity of the total characteristics are reflected in a large number of users' entry, access, drop of object, the request failed and the session application, so as to dramatically enhance the occupancy value of CPU.

3.2.2Judge abnormal interval

In the specific application of the system, the method of variance analysis is used as a statistical analysis model. And based on the similar value and the abnormal value in the statistical interval to finish feature data analysis and monitoring analysis. And then according to the reference value and the variance contrast to determine the abnormal range.

Based on the statistical scheme, setting up the adaptive strategy with the abnormal interval threshold.

CONCLUSION

This paper designs a database security audit system based on security. Compared with the traditional audit plan, the paper has the following advantages: visualization of global configuration, simplified model and enhance the universality and the expansibility. And uniforming audit record format can solve the problems of data redundancy and data overflow. While setting up exclusive channel of data query can realize real-time monitoring and identify potential attacks. On the basis of the existing log protection module, it can reduce the impact of security audit on database performance, reduce the proportion of its memory and improve the system security greatly, which means it is a better direction of development for research.

Reference

[1] Huang Fang. A new database system protocol audit model [J]. computer engineering and application, 2014, 40 (17)

[2] Bishop M.Goal oriented auditing and logging[J].IEEE Transaction on Computing systems, 2006.