Exploration of database security audit protection system in Universities

Rao Yan[1,a,#], **Zheng Yuan**[2,b,*]

[1]Modern Education Technology Center of Guangdong Pharmaceutical University, Guangzhou, China

[2]Guangzhou University of Traditional Chinese Medicine Information Center, Guangzhou, China

[a] ry@gdpu.edu.cn, [b] zy@gzucm.edu.cn

[#]First author, *Corresponding author

Keywords: Data security; database; security audit

Abstract: With the introduction of network security law, data security law, personal information protection law and other network information security laws and regulations one after another, the importance of national data security protection has been brought to a new height. As a key infrastructure for storing and managing core data in various information systems of universities, database monitoring and auditing as well as security protection are particularly important as it keeps important and sensitive data assets. This paper takes database security audit as an entry point to discuss the difficulties encountered by universities in the process of planning and construction of database security protection system and its ideas to cope with them, and further improve the data security protection system of universities by taking measures such as real-time database security audit and risk control on the basis of guaranteeing the continuity and availability of information system services.

1. Risks and challenges of database security

With the deepening of digital transformation construction of colleges and universities, they have deployed and used information systems of teaching, scientific research, academic work, personnel, finance, assets, procurement, etc., and accumulated a large amount of teaching, scientific research and management data and shared and utilized them through data governance platform, and the value of data has been tapped, which has provided a lot of convenience to teachers and students in their study, work and life, fully reflecting the service concept of "more data, less legwork". The service concept of "data run more, teachers and students run less" is fully reflected. However, while the data facilitates the service management of universities, it also lays the hidden risk of data security, such as the deletion, leakage and tampering of important data caused by the irregularities in the daily operation and maintenance management and operation of various information systems, which often happens. How to implement the protection of confidentiality and integrity of important data under the premise of guaranteeing the availability and continuity of important data has become an urgent problem to be solved by the information security management department of universities.

In recent years, due to the continuous in-depth network security level protection work and the implementation of security rectification work, in terms of data auditing, it used to rely more on the permission control of the database software itself and the log audit function, which solved the problem of data auditing to a certain extent, but there are also many drawbacks:

(1) Business performance impact. Data exchange and processing, open the database software comes with the audit function may affect the performance of the database itself, and may even affect the continuity and availability of information system business;

(2) Local log storage is at risk. Data logs are stored centrally in the local database, and the negligence of the third-party operation and maintenance or developers in management may easily cause the risk of off-base, deletion and data leakage. In addition, the log files of the database system itself has the security risk of being deleted or tampered with, making it difficult to truly safeguard the integrity and authenticity of the database log audit information;

(3) Difficult to locate the source of traceability. A single means of network security and database

DOI: 10.25236/icfmhss.2023.020

access control can hardly meet the control of sensitive data access, and improper setting of database operation rights by database administrators or leakage of database user login password will lead to database data tampering or leakage, which cannot be easily found in time, making it difficult to trace and locate security events.

(4) It is difficult to monitor in real time. Traditional data center network security equipment, such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), operation and maintenance bastions, etc. are difficult to monitor in real time to find out the unauthorized access, data tampering and sensitive information leakage in the process of database operation and other behaviors to issue alerts.

(5) Intelligent analysis is not effective. Database software itself comes with the log audit function is difficult to visualize the intelligent analysis of various types of database operation behavior.

In response to the above problems, the current common practice is to independently deploy database security audit system (DAS, Database security Audit System) to solve the daily fine-grained data access audit, accurate database operation behavior backtracking and real-time grasp of the important database operational status visualization, and through the set database security behavior Through the set database security behavior rules, the threatening operations can be timely warned and blocked, so that the daily operation of database can be monitored, dangerous behavior can be controlled, access behavior can be audited, and security events can be traced [1].

2. The deployment of database audit system

At present, the database security audit system generally adopts the following two ways to carry out security audit on database operation behavior in a comprehensive manner:

(1) Audit analysis based on log archiving. The main coverage of the representation layer to the application layer in the OSI seven-layer network model, using keywords to analyze the semantics of the entire statement of the operating database, and as much as possible, the SQL statement of the operating database is fine-grained parsed to meet the precise detection, response and audit for various violations [2].

(2) Behavioral audit analysis based on network traffic. The main coverage of the network layer to the session layer in the OSI seven-layer network model, according to the network interface to be listened to, IP addresses and network ports and other information on the network port to capture database traffic, and use the analysis of the original IP messages of database access to achieve audit statistical analysis of database access behavior [2].

The traditional deployment method is more often through the network traffic mirrored on the data center network transmission equipment through the bypass to the database audit equipment for log analysis, and this approach requires the database audit system to achieve automatic identification of different types of databases through the collection and data analysis of database network traffic, using the respective characteristics of each database type private communication protocol [3]. However, audit monitoring is performed purely from the network traffic of bypass mirroring, but monitoring of the local database access operation records of the information system is not possible, so the precise traceability of risk behaviors is more missing, and it is difficult to ensure the integrity of audit monitoring.

In order to ensure the accuracy and integrity of database security audit logs, the mode of lightweight deployment and installation of Agent plug-in on the operating system where the database is located will be adopted to realize database security audit (as shown in Figure 1), firstly, database operation and maintenance managers will unify the IP addresses of the target asset database to be monitored into Agent by setting security policies on the database security audit system, and then deploy and install Agent plug-in in the database server system to realize the collection of access traffic and forward it to the database security audit system for unified analysis. Management, and then deploy and install Agent plug-in in the database server system to realize the collection of access traffic and forward it to the database security audit system for unified analysis.

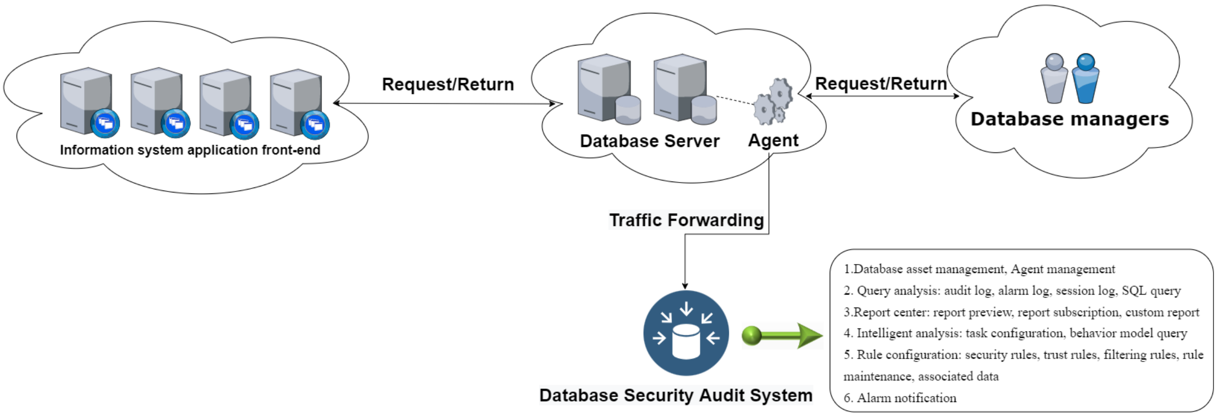
Information system application front-end
Request/Return
Database Server
Agent
Request/Return
Database managers
Traffic Forwarding
Database Security Audit System
1.Database asset management, Agent management
2. Query analysis: audit log, alarm log, session log, SQL query
3.Report center: report preview, report subscription, custom report
4. Intelligent analysis: task configuration, behavior model query
5. Rule configuration: security rules, trust rules, filtering rules, rule maintenance, associated data
6. Alarm notification

Figure 1 Database audit agent agent deployment model

The use of database audit agent deployment mode not only solves the problem of database audit and monitoring log integrity, but also refines the configuration of database related security rules and policies to the specific single database to be monitored, so that all kinds of databases can be easily monitored and managed centrally and uniformly, and provides database security administrators with complete database audit analysis, leak trajectory analysis, database access relationship visibility, and database security management through refined audit reports. Through refined audit reports, it provides database security administrators with complete database audit analysis, leak trajectory analysis, database access relationship visualization, database attack threat analysis, which can timely discover the use, flow and risk of data assets, and data relationship diagrams help restore access trajectories when tracing, and meet the compliance requirements such as network security level protection while satisfying comprehensive, efficient and easy-to-use auditing.

3. Operation and maintenance management of database security audit system

After completing the deployment of database security audit system, firstly, the data audit authority is reasonably controlled through the mechanism of separation of powers, effectively planning, allocating and managing the use of data audit by managers, dividing the authority of administrators, auditors and operators in the database audit system, stipulating that each role user can only operate the database audit system within the scope of its authority.

In the process of database audit system operation and maintenance management not only to achieve accurate records of database operation behavior, but also to ensure the business continuity and availability of information systems, to achieve real-time database security risk alerts and improve the efficiency of risk disposal. Its operation and maintenance management mechanism is mainly based on sensitive data, policy, data flow baseline and other dimensions, the production flow of data, data operation monitoring, auditing, analysis, timely discovery of abnormal data flow, abnormal data operation behavior, and risk alert and report output. Its operation and maintenance management is mainly reflected in three aspects.

(1) In advance Pre-audit.mainly based on prevention, the database assets are sorted out in detail, including database asset names, database types and versions, database software operating system types and versions, database IP addresses and ports, database assets are imported into the database audit system, and security risk detection-related tasks are added, such as: each database behavior model analysis tasks, analysis reports, and administrators perform security analysis and reporting through security analysis of the relevant analysis and report situation, to optimize the adjustment of relevant security policies.

(2) In-fact alerting. The data audit system basically has effective identification of CVE and other vulnerability library feature detection, SQL injection attack, password cracking, login abnormalities and other database security detection functions to achieve real-time monitoring and comprehensive coverage of database attacks and various types of risky operations, including suspected attack risks, bulk dragging library risks, highly sensitive data leakage, sensitive information tampering, once the

discovery of data leakage and damage that may lead to Once malicious behaviors are found that may lead to data leakage and damage, the database audit system will issue threat alerts by email or SMS in time, and the operation and maintenance managers can quickly locate the relevant alerts and block them in time for the threats.

(3) Traceability afterwards. After a data security event occurs, the log information recorded by the audit mechanism can be used to trace the source of the event, realize the linkage of the server IP in the risk alert, collect detailed information such as the name of the data asset application involved, database type, source address and destination address of SQL statement operation, help the operation and maintenance personnel trace the source accurately, restore the process of the event, and provide reference for the post-event rectification and defense strategy. It helps operations and maintenance personnel to accurately trace the source, restore the event process, and provide reference for post-event correction and defense strategy.

4. The next step of optimization

Although the deployment of database security audit system can solve the problem of data security audit, but also encountered some technical difficulties in the planning of the deployment system to achieve full coverage, still need to take different solutions for different problems.

(1) Operation and maintenance operations and applications between the traffic difficult to distinguish the problem and solutions

A large number of information systems between the normal access traffic and daily operations and maintenance operations traffic mixed together, seriously interfering with the audit of operations and maintenance operations. This requires the establishment of a multi-dimensional traffic filtering strategy for access sources, users and access tools to accurately distinguish the operational behavior of access to the database, filtering audit logs that do not require too much attention, avoiding unnecessary waste of resources and human energy consumption.

(2) Server local access to the database source address is difficult to trace the problem and solutions

When the operation and maintenance personnel access the database locally on the database server, the logs usually only record the IP address of the server local machine and take it as the source address, and cannot record the address of the operation and maintenance terminal. In this way, it is necessary to further use the function of advanced collection of source address or incorporate the unified monitoring and maintenance of remote operation and maintenance fortress machine, and the database security auditors can see the terminal address of the initial implementation of the login to achieve accurate traceability of the operation and maintenance operation scenario after the operation and maintenance personnel access the database directly from the server local.

5. Conclusion

The construction of data security system is not an overnight project, and the construction of a comprehensive audit system for the whole chain of data business access can make the data flow present a visual data relationship and a comprehensive understanding of the security status of data assets. In the process of monitoring data security operation, it is also necessary to further combine data classification and classification to conduct a comprehensive audit of the operation of business application systems and database systems. In the process of digital transformation and data security governance going hand in hand, universities have to deploy database security audit systems in combination with the use of data situational awareness technology to do a good job of data security auditing and risk warning. With the development of artificial intelligence, the detection capability of database security audit and situational awareness machine learning will be further improved to cover various database risk scenarios, optimize the timeliness and effectiveness of policy monitoring alerts, and better build a credible and controllable digital security barrier for the university.

References

[1] Fan JY. Research on the application of database security audit system in higher education [J]. China New Communication, 2019, 21(18):42-43.

[2] Wang Xin, Li Hengjie. Design and implementation of database security audit system[J]. Industrial instrumentation and automation devices, 2016,(01):86-89+93.

[3] Yang Lei, Bi Hongjun. Database security audit system based on bypass listening [J]. Computer Engineering and Applications, 2015, 51(8):138-142.