Research on SQL Server Database Security

Du Fang, Zhang Kaiyuan, Qian Jin
NonCommissioned Officer Academy of PAP, Hangzhou, Zhejiang, China

Abstract: Database security mechanism management, is the main link of virtual information communication protection. Only in the case that the security of SQL Server database application can be guaranteed, it can better accomplish the work of storing and calling data. Based on this, this paper analyzes the security regulation technology of SQL Server database from the three aspects of login, transmission and application, researches and analyzes the main module of database in the database application, carries out a comprehensive and in-depth exploration of its security, analyzes its security on this basis and proposes the methods to improve the security when the security is insufficient to achieve the point of clarifying the protection of the program and promoting the computer industry. The purpose is to clarify the main points of program protection and promote the scientific development of the computer industry.

Keywords: SQL Server Database; Application Programs; Database Security

1. Introduction

Database applications in the operation of the application program, based on the current WINDOWS system development or with the help of the rest of the development system selection, to achieve all kinds of security work. Although security has been emphasized, there are still security risks, and it is necessary to solve the security problems in the future, so that it is in a safe and stable state of operation. The SQL data service system is the most important program manipulation processing structure in the current computer structure, which realizes the associated operation in virtual information interaction, communication and exploration. In order to ensure the gradual optimization of the smoothness and consistency of SQL Server database development, it is necessary to do a good job of security control and protection strategies in the process of program exploration.

2. SQL Server Database Security Login Mechanism

SQL Server database, is the main window of computer information storage and management, its security protection system is analyzed from the perspective of program operation security on the one hand, on the other hand, it is discussed from the level of system information storage security, for this reason, from the moment the program is started, the implementation of security protection, is the SQL Server database program protection of the first protection gate - SQL SQL Server database security login mechanism.

According to the current computer SQL Server database program design, the login link protection is mainly divided into two parts: program authentication and SQL Server database authentication. The former is a security check with the login authentication structure of the web interface. For example, when we start the database, we need to fill in the "login user name, login password" and other information, which are the security management methods of the SQL Server database program authentication part; the latter is mainly the security verification of the SQL database part, which is mainly verified by the SQL database input command in the program. This part is mainly verified by the level of matching degree of SQL database input instructions in the program. For example, in the process of SQL Server database operation, when the program searches the database, it will not be able to output the test results when the local statement is inputted incorrectly; or, some of the high-level files will be locked up, and the user needs to be verified again inside the SQL Server database before obtaining the information, which are the representative forms of the verification of the SQL Server database according to the full login. In the actual operation process, the security verification of the SQL Server database login link should pay

attention to the comprehensiveness and convenience of the initial login mechanism verification test, so that the SQL Server database can be utilized to provide customers with satisfactory services on the basis of strengthening the protection of the virtual environment information storage.

3. SQL Server Database Operation Security Mechanism

SQL Server database is manipulated and operated by various kinds of object statements, in order to strengthen the security of program instruction operation and avoid virus interference in virtual space, different databases can be given separate security instruction manipulation protection. Combined with the current data manipulation practice requirements in the use of SQL Server databases, the security protection in the operation process can be divided into three aspects: object operation security mechanism, statement operation security mechanism, and built-in data rights [2]. Among them, the object manipulation security mechanism, the SQL Server database is mainly analyzed by the object control as the main body, and in the SQL statement query, update, insertion and other links, the corresponding authorization security judgment is carried out. For example, if users want to query the data information related to "apple", they need to set the "Select (query)" command, and then input the conditions related to "apple". The query software begins to analyze the security of the objects operated by the query control. If the control operation is safe, the system will continue to execute the command; otherwise, the system feedback security prompts, the process is the SQL Server database object rights security protection mechanism operation of the embodiment.

The statement operation security mechanism refers to the statement operation security protection in the process of table creation and view construction during the operation of SQL Server database.The common statement operation security analysis in SQL Server database is mainly used in the two modules of table creation and view access. When a customer uses SQL Server database for financial data table statistics, the condition of table analysis is set as "February Financial Income and Expenditure Detail Table".When the SQL Server data program command is running, the security protection mechanism will analyze the current data output after the program retrieves the data according to the condition. The security of the window and the reliability of the statement operation. Once the test data does not match with the subsequent information, the SQL Server database will automatically stop the information transmission and jump out of the command interface, which is the security demonstration of the authority of the SQL Server database operation statement.

The internal security protection system of the database is also a part of the operation security control. It mainly analyzes the reasonable situation of the operation command of the data command object, or it is grasped from the level of coordination of the operation of the database structure command. For example, SQL Server database instruction information and so on, these are the program safety operation protection form.

4. SQL Server Database Network Window Security Mechanism

SQL Server database is the main resource protection system of computer information processing and manipulation, and its operation coordination and analysis effect will directly affect the data structure. For this reason, to strengthen the safety management of digital program operation, should also pay attention to the analysis from the data window practice. That is, the SQL Server database network window security mechanism is the protection of virtual information communication transmission link.

For one thing, the SQL database can use encryption cipher method to protect the security transmission network. For example, the common SSL protocol transmission channel in the computer, etc., are encrypted database operation form; Second, the database IP restriction conditions. That is, in the SQL Server database network data communication process, strengthen the data transmission in the security protection mechanism strategy of hidden danger control, can circumvent the IP address in the hidden data information network security protection is not in place, it is the most coordinated and sustained data security grasp in the security protection way. Third, the detection of security instruction terminal technology. That is, during the security protection and processing of computer networks, a core data

communication and supervision channel can be introduced on the basis of the overall network program, and then with the help of professional detection and supervision ports, the terminal hidden protection of the SQL Server database is also an effective way of network security protection. Fourth, virtual security backup protection. Although the database has established multiple security protection systems in its operation system, the extensibility and expansibility of virtual space features will still increase the problem of database manipulation, for this reason, the implementation of orderly backup regulation is also an indispensable form of network transmission security protection in the process of its work practice.

5. Main Modules of the Database in SQL Server Database Applications

5.1 User Access Functions
Two login authentication methods are set in the user login, one of which is WINDOWS authentication mode and the other is hybrid authentication mode. The former can only use WINDOWS authentication identity, so that users can only use WINDOWS account for network authentication. The latter can use WINDOWS to complete the authentication process, and with the application of the relevant account to achieve specific authentication work, and ultimately the quality of the entire system to obtain a substantial improvement in the operation.

5.2 Network Connection Function
The network connection usually uses a proxy server to connect with the relevant programs and the Internet's comprehensive server, the process needs to set up the corresponding network transit station, and the establishment of a buffer, in order to realize the rapid analysis of various types of data.
The process can be better accomplished for the protection of data and information, in addition to connecting the process of the signal needs to pass through the transit and firewalls. The purpose of the firewall is usually to better complete the inspection and analysis of data, especially through the firewall and the server work together to better improve the operational security of the entire system.

5.3 Role Management Functions

Role management involves user registration and user activation of two work items, the former in the process of practice, the user is required not only to submit personal information, but also need to set up a password for the subsequent login process to lay the foundation [1]. The latter for the user to better have the relevant rights, and in the role of the activation process, the need to use the database program to activate the user information and limit the user's operating privileges, but also to clarify and modify the user's work in the process of the various types of rights.

5.4 View Display Function
The view display will realize the in-depth protection of the information displayed in the database through the adjustment and setting of all kinds of access privileges and data usage, in order to maximize the security of the database. However, from the point of view of the role of the entire system operation, the user of the view can only query and modify the way to complete the access to all kinds of information and the use of work.

6. Database Security in SQL Server Database Applications

6.1 User Access Function Security
The security of user's access function refers to a series of technical and management measures to ensure that only authorized users are able to access specific resources, such as data, applications, etc., and at the same time prevent unauthorized access and data leakage. Among the methods of securing user access security, firstly, users can deeply prevent others from impersonating the relevant privileges of this registered user by setting independent passwords to improve the security of the whole system. Secondly, in the password verification, we also record and analyze the wrong password information to know whether there is any security problem of the account, and improve the operation security of the whole system through the effective solution of this problem. Finally, the user rights are activated in accordance with the set functions, and when the rights can better complete the management and optimization of more projects, the rights of the system can be fully guaranteed.

6.2 network Connectivity Security

The security of network connection function is of great significance for protecting personal and enterprise information assets, maintaining network security, and reducing cybercrime activities. With the development of technology and the expansion of network applications, the importance of network security will be more prominent. There are certain problems with the security of network connection, especially for the way the server is connected or when the firewall is not established, the whole system is vulnerable to malicious attacks by attackers, so in order to improve the security of the operation of this system.

First, through the establishment of a transit server to complete the screening and investigation of various types of data, the work in the implementation of the process should be carried out by the relevant staff through the use of the final construction of the system, so that the server system on the data sources to accurately analyze the data so that such data to play its due role in ensuring that all types of data to ensure that the network connection can be safe and stable. The second is the completion of the corresponding firewall system, the construction of firewalls, including physical firewalls and software firewalls, under the joint role of which can further improve the accuracy of the analysis of data.

6.3 Role Management Functionality Security

Role management security issues are usually human factors, in fact, the database application itself has a very high level of security performance. In specific use, the staff is required to increase the complexity of the password, and not to transfer the relevant rights to illegal accounts or accounts that do not have the rights. In addition, the enterprise should complete the unified jurisdiction and issuance of all kinds of high-privilege accounts, and when the account password leakage problem occurs, the account holder will be held accountable.

6.4 Security Of View Display Function

The view display function can be said to be the most secure item in the whole system, because it can only complete the analysis and display of various types of information [2]. Usually for all kinds of stored information to complete a separate analysis and clear work, and the rest of the staff can not understand and observe the

information to obtain business secrets. In addition, the view display system because of its own low complexity, so it can better complete the mechanism of all kinds of information adjustment work, greatly reducing the chances of security accidents.

Conclusion: In summary, the SQL Server database application in the operation process, its security is manifested in the view of higher security, lower risk of user registration, etc., and for some of the problems in the system, it can be completed through the improvement and optimization of the system, in which the most core items are built into the transit server and the firewall, through the use of which can ensure that the security of the entire system is improved. The study of the security mechanism of SQL Server database is a theoretical generalization of the digital application method. On this basis, the program security protection means are analyzed through SQL Server database security login mechanism, operation security mechanism and network window security mechanism. Therefore, the results of the article bring a guiding tendency for the innovative development of the database.

References

[1] Gao, See-Bin. Taking SQL Server as an example to discuss the construction of database security mechanism[J]. Shandong Industrial Technology,2018(10):150-151.

[2] Zhu Chao. Research and Discussion on SQL Sever Database Security Mechanism[J]. Science Popular(Science Education),2018(08):186.

[3] Wan Shuai.Research on database security in SQL Server database applications[J]. Computer Fans,2018(06):82.

[4] Zhang Jie,Yuan Litian. An Introduction to Database Security in SQL Server Database Applications[J]. Digital technology and application,2017(08):203+205.

[5] LIU Changqing,DANG Lina,ZHANG Li,et al. Discussion on the integration of Civic and Political Education in the course of "Bioengineering Equipment"[J]. Industry and Technology Forum,2022,21(11):139-140.

[6] WU Shujing,WANG Jingguo,WANG Yuanqiang,MEN Yong,LIU Xijian. Exploration of teaching reform led by course ideology[J]. Shanghai Chemical Industry,2024,49(02):49-51.