Advances in Computer Science Research, volume 80
International Conference on Computer Science, Electronics and Communication Engineering (CSECE 2018)

Design and Implementation of Database Centralized Access Control and Audit System

Ying Zheng[1] and Qinghai Bai[2,3]
[1]Journal Editorial Department, Inner Mongolia University for Nationalities, Tongliao, 028000, China
[2]College of Computer Science and Technology, Inner Mongolia University for Nationalities, Tongliao, 028000, China
[3]Institute of Computer Application Technology, Inner Mongolia University for Nationalities, Tongliao, 028000, China

***Abstract*—This paper explores the Oracle database security access control's implementation strategies, including: realize the centralized access control to the distributed Oracle database and audit through centralized policy configuration; realize the security access control to the Oracle database through encapsulating PL/Sql Developer database management tools, without changing PL/Sql Developer tools' database DBA operating practices; the system can configure the database management strategy based on different DBA roles or database users so that different DBA role can access to different database schema or a combination of database schema, realizing the SQL script review and audit.**

Keywords—oracle database; security access control; audit

I. INTRODUCTION

The Oracle database is one of popular databases used by large enterprises [1, 2]. This paper explores the Oracle database security access control's implementation strategies. Its main functions are as follows.

(1) Realize the centralized access control to the distributed Oracle database and audit through centralized policy configuration;

(2)realize the security access control to the Oracle database through encapsulating PL/Sql Developer database management tools, without changing PL/Sql Developer tools' database DBA operating practices;

(3)the system can configure the database management strategy based on different DBA roles or database users so that different DBA role can access to different database schema or a combination of database schema, realizing the SQL script review and audit.

After the system implementation, all the passwords, including the database servers', the application server operating systems', and the database systems', are under the unified administration of the system and specialized operating maintenance department.

If the scrip needs approval to perform, then submit the approval first. If the script requires audit, then perform the audit. It can set a period of time when no operations of database are permitted.

The database operation and maintenance team, under the administration of the database manager of the operation and maintenance department, is in charge of all the operation and maintenance of the database system.

II. THE TYPICAL OPERATION AND MAINTENANCE PROCESS ANALYSIS

As an IT service company engaging in database operation and maintenance for many years, a typical outsourcing database operation and maintenance client has a similar organization structure [3, 4]. However, this organization structure has the following drawbacks. First of all, the client DBA cannot manage all production databases by artificial means, since even the routine maintenance also requires a lot of effort (for example, change passwords and backup scrips for all databases). Secondly, the client DBA does not know what operations have been performed on the production database. Thirdly, the Operation &Maintenance Company's professional DBA and the Development Company's engineer do not develop a good combination. If the operation and maintenance DBA can assist the development engineer to review all executed SQL statements or scripts, it is able to reduce a lot of potential problems [5].

Implementing this system can effectively solve the above problems.

In a production environment, all production databases will be recorded into the system as data source. Client, Operation &Maintenance Company, and Development Company, as different roles, will be given various permissions (DDL, DML, DCL, etc.), corresponding to the actual situation and the individual data sources. Mapping the roles and the data sources can effectively mask the actual accounts and passwords of the production database, preventing the leakage of passwords. When the Operation & Maintenance Company or the Development Company's staffs execute the SQL statements, these statements will be sent to the end for the audit of client DBA. Only through passing the audit, can the SQL statements and scripts be executed in production environment. At the same time, the client DBA can assign a trusted Operation & Maintenance DBA to help complete the audit.

After a series of system implementation above, it in nature represents a reform of operation and maintenance management.

III. THE PROCESS OF USING THE SYSTEM

A. The Running Process

Through the massive open-source database audit, the database management and data source management can add the production database as well as its users and passwords that need to be managed to the massive open-source database audit software.

Through user management and role management, it can add the company and its employees that need to be managed to the massive open-source database audit software.

Through the role data source function of the system, it can establish the mapping of database users and database accounts.

After completing the above work, the system can be put into operation.

B. Log in the System

Open the IE browser and enter the address in the address bar to log in the page. Enter the username / password and log in the system homepage.

C. Database Management

In the database management tab, add all the production databases to the system.

Click the "Add" button and fill in the relevant information. For example, enter the database name A1_ODS, URL (THIN mode) jdbcOracle:thin:@192.168.1.60:1521:al_ods.

Instructions as follows:

The string format of URL (THIN) mode is: fixed string (jdbc: Oracle: thin:)@database IP address: Port: Service name.

RUL (connection string) is the DESCRIPTION part of tnsnames.ora file, such as:

(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.1.60)(PORT=1521)))(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=ods))

It will return to the list page after a successful registration of production database.

D. Data Source Management

Data source management is to achieve the function of allocating and managing the operation rights of all database accounts and passwords.

Click the "Add" button to add the database user information.

The suggested naming rules for data source name field are as follows: example name_username_utility (company name). For example, ods is the example name, scott is the database user name, and dev refers to development. It can easily be classified and managed through standardized naming.

Database fields can by automatically selected, without manual entry.

The username and password fields are the sys system administrator's account and password.

The purpose field is a descriptive field and can be filled according to the actual situation.

The access time field needs to be filled out similarly to the UNIX system's cron tab command. It can limit user's access time to the database by setting time limits.

The database user permission level field can be used to configure the system whether it records users' operations, whether audit the statements containing the keyword (for example, update, insert……), whether open some functions of PLSQL DEV.

When the database information is incorrect or fill out the wrong password, the system will alarm errors.

After adding the sys users, we can repeat the steps above and add other users to the massive open-source audit software.

Note: The sys users should be added first.

E. Role Management

In the customer's organizational structure, each company is responsible for different task, including development, maintenance, and monitoring. Therefore, different company may play a different role.

Click the "Add" button and add the privilege information of the role.

Fields explanations are as follows: the user's role name should be filled by following the "example name_role type" format. Select the appropriate privileges for roles based on actual conditions.

F. Role Data Source

The role data source is to carry out the roles and corresponding database accounts. After establishing the role data source mapping, all operators who belong to certain role can only use the corresponding database account to operate the database. Meanwhile, the privileges of the operator are limited by the privileges the role and the database account. His or her operations will be recorded and audited by the system.

Click the "Add" button and add the role management data source information page.

Fields explanations are as follows: the role field is the established role; the data source field is the established data source user. The two fields are not required manual entry. You can select them from the list.

Click the "Submit" button and return to the role data source list page.

G. User Management

User management is to register and record the specific operator according to his or her role (or company).

Fields explanations are as follows: the user name refers to the English code of the operator; the full name can fill out the

real name of the operator; the user group is the operator's company; the professional status is the operator's specific job position; the user's role is the operator's database account; the log-in password is the password of operator using pl/sql dev.

Click the "Submit" button and return to the user list.

H. Approval Management

The approval management includes pending PL/SQL, approval implementation records, approval return records, approval implementation records (30 days ago), approval return records (30 days ago), and other functional modules.

The system will execute the SQL statement in three statuses: the status of submission, the status of approval, the status of approval return.

When an operator executes a SQL statement, if the statement has the key word of "approved", the operator could not execute the statement in the production system. The statement needs to be approved by customers. Its status should be "submission".

When a client DBA believes that the submitted SQL statement can be executed, he or she will give approval and the statement will be executed by the operator. Otherwise, the operator cannot execute the statement.

Click the hyperlink column in the "Title" list and enter the approval page.

Under normal conditions, only the client DBA can carry out the approval. The operation and maintenance DBA can review operations. "Approval" means all approved SQL statements can be executed. The reviewed SQL statement still needs approval before implementation. By means of this arrangement, the operation and maintenance DBA can take advantage of their professional skills and provide a reference for client DBA decisions.

The client DBA can also give full authorization to the operation and maintenance DBA for approval. Thus, it can reduce the workload of client DBA. The client DBA can concentrate on the more important production system.

After the approval, you can check the approval records.

Click the hyperlink column in the "Title" list and enter the details page.

After the operator executes the statement, it can be found in the approval execution record page.

The approval return records save the SQL statements that the client DBA did not give approval of execution. These records indicate that the returned SQL statements may make mistakes or potential risks in execution.

I. Audit Management

The audit management module is the system audit logs, including the following three aspects: database audit logs, system operations logs, and system log-in logs.

The database audit logs record the execution of SQL statements, including the executor, database, database account, application time, status of SQL statement and result.

Click the"Notes"hyperlink and view the detailed process of the application, approval, and execution of the statement.

The system operations logs record the history of user using the massive open-source database audit software. The massive open-source database audit software can automatically save the user name, IP address, operating contents, operating results, date, and so on.

The system log-in logs record the history of user logging in the massive open-source database audit software. The massive open-source database audit software can automatically save the user name, IP address, date, and so on.

ACKNOWLEDGMENT

This paper Supported by Inner Mongolia Colleges and Universities Scientific Research Projects (NJZC16191) and Dr. Scientific Research Fund of Inner Mongolia University for Nationalities (BS323).

REFERENCES

[1] Chen jing,Fan naiji,Yuan xiaodong,Jiang yilan.Oracle database access technology under Matlab environment [J](in Chinese). Journal of Computer Applications, 2015,S1:78-82+97.

[2] Ni jiaming,Han qiang.The design of power Information System data recovery system Based on Oracle Database [J] (in Chinese). Electrical Applications,2016,12:74-76+81.

[3] Guang baohua,Jia fengwei,Wang tianjing.The database access control policy based on the properties for Cloud storage platform [J] (in Chinese). Computer Science,2016,03:167-173.

[4] Zhu yi,Zhu hong,Xie meiyi,Feng yucai.Mandatory Access Control formal analysis and proof for Database Management System [J] (in Chinese). Computer Systems,2015,03:401-407.

[5] Wang zhenhui,Wang zhenduo,Xie yingbai,Zhi kanmai.Web Database Security Middleware Research and Design Based on XML [J] (in Chinese). Journal of Computer Applications and Software,2015,08:38-42+179.