Oracle Database Permissions Reinforcement Exploration AndSecurity Maintenance

Xuan Xia, Hean Liu
College of Science, Hunan City University, Yiyang, 413000, China

Abstract: With the development of society and the improvement of people's living standards, the data of life has come, but with the rapid development, the database security performance is particularly important. In the database security configuration, relevant safety reinforcement work is needed. To confirm the safety of the database, however, if the configuration information connecting to the database fails or is not modified in time, the consequences are very serious.

Keywords: Oracle permission; Database management; Database security maintenance

1. Introduction

As one of the most popular databases nowadays, Oracle database is widely used. But there are some loopholes in its safety management. Oracle database security management is mainly based on network and user operation as the leading factor. At present, most of the IT enterprises have their own databases, which store the data in the database to achieve the purpose of resource sharing and data sharing [1-3].

In the current Oracle database, when object access is allowed, the system defaults to three types of permissions: object type, system type, role type [4-5].

Orace-object type: is the embodiment of object-oriented programming, which encapsulates the database structure used to manipulate its procedures and functions. It consists of two parts: object type header and object type body. Object type headers are used to define common attributes and methods for objects; object type bodies are used to implement the previous step. Oralce - System type: Users can only log in to em as normal unless you grant it system privileges of sys DBA. Oracle - role type: Users can authorize roles, and system and object permissions need to be authorized separately.

2. Rights Management

2.1. Landing of oracle database

With the rapid development of computer technology and information technology, Oracle database has also ushered in a broad application prospects. at present, most enterprises are in the Oracle database based on the establishment of their own enterprise network, the data will be stored in a unified data, to achieve resource sharing. Network system is particularly important in Oracle database, and network system has variability. Therefore, in order to optimize the Oracle database, we must optimize the database on the basis of the network system. Although the network system is not the internal system of Oracle database, but the impact on Oracle database security management is more profound, the database function depends on the running state of the network system, the two are in direct proportion. In order to avoid the normal operation of the database, the security administrators must optimize the security protection function of the network system under the condition of ensuring the smooth operation of the network system. Investigation shows that most of the factors affecting the security of database management come from external factors, hackers and other use of technical network defense system attacks to obtain the desired data and information. In order to optimize the network system, firewall settings are very necessary; it can detect the network timing, to protect the security of oracle database inside and outside. Its biometric identification system can effectively deny remote access to DBA, so password security will become a thing of the past. I think that in the future security technology, building a dual effective firewall has become the key to overcome security vulnerabilities, privacy leaks without delay. Double or even multiple can give a great leap in security performance.

2.2. Oracle entity permissions and System privileges

When a user is allowed to access an object or execute a program of another user in an oracle privilege, permissions can be granted to the user public or role, and if a privilege is granted to a particular user, it indicates that the user is unconditionally trusted (where the privilege is Oracle itself and can be defined)).Entity privileges refer to the access of a certain privilege user to a table or view of another user for a table or view. The system permis-

sions are user rights defined by the database itself. We need to pay attention to several aspects of system privilege management classification. The first is DBA (the highest permissions of the system itself, which represent the permissions of the database structure). DBA permissions can only be granted by DBA users (connect, resource, DBA permissions). The second is Resource (it's worth noting that privileged users can only create entities, not database structures like DBAs). The third is Connect (which is a relatively low-level privilege and can only be logged on to oracle, and cannot build entity and database structures with the above two privileges).System predefined roles: System defined roles are common roles that are automatically created by the system when the Oracle database is created, and these roles have been granted permissions by the system. DBA can directly use predefined roles to authorize users and modify permissions of predefined roles. There are more than 50 predefined roles in the Oracle 11g database. The following table lists several commonly used predefined roles and permissions.

Table 1. Oracle database allows users to create, modify, delete roles, and grant and reclaim permissions for roles

Role	Authority
Connect	Create. session
DBA	Contains all system privileges, with the with_admin_option, to grant system user privileges to other users
Exp_full_databast	Role：Execute_catalog_role and select_catalog_role Object permissions ： sys.incvid,sys.incfil and sys.incexp.inser(delete,update)
Imp_full_database	Contains all the permissions and roles required to complete database import.
Resource	Create cluster,create indextype,create operator,create procedure,create sequence,create table,create t rigger,create type

3. Role Management

A role is a set of permissions assigned to a user who has all the permissions in that role. System predefined roles are some commonly used roles automatically created by the system after the database is installed. Next, let me briefly introduce these predetermined roles. The permission contained in the role can be querying with the following statement: Sql>select * from role_sys_privs where role='role name'; CONNECT, RESOURCE, DBA: these predefined roles are primarily for backward compatibility. It is mainly used for database management. Oracle recommends that users design their own privilege plans for database management and security rather than simply using these predetermined roles. These roles may not be used as predefined roles in future releases. Delete_ catalog_ Role, Execute_ Catalog_Role, Select_ Catalog_ Role: These roles are primarily used to access data dictionary views and packages. Exp_ Full_ Database, Imp _Full_ Database: these two roles are used for data import and tools. Aq _User_ Role, Aq_ Administrator _ Role: Aq: Advanced Query. These two roles areused in the Oracle advanced query function. SNMPAGENT: for Oracle Enterprise Manager and Intelligent Agent Recovery_ Catalog_ Owner: used to create users with recovery libraries.

For information about restoring the library<< refer to the Oracle document "Oracle9i User-Managed Backup and Recovery Guide">> Hs_ Admin_ Role:<< A DBA using Oracle's heterogeneous services feature needs this role to access appropriate tables in the data dictionary >>

4. Safety Maintenance

System stability optimization User operating system is a direct impact on the security of Oracle database, and the security risks are large. Users in the operation process, in order to keep the system running steadily, establish the role of the same type of users and centralized management. Distinguish permissions between users, and then set various roles, permissions, or part of the content is not accessible page settings. System administrators design user rights according to user's habits and optimize user operating system. Oracle database management system is divided into Connect, Resource, DBA three kinds, are temporary access, multi-page access and enhanced database management. This management mode can reduce the difficulty of work.

User control. When users access the database, they first need to log in the account or input dynamic commands. Only by resetting the access rights can users read the information in the database. This method can not only prevent external users from destroying the database artificially, but also prevent unrelated people from accessing the database arbitrarily, thus avoiding some problems. Necessary threats, the use of user management mode to protect real users, but also by optimizing the user account management system, optimize the user authorization system, optimize the role management system to maintain Oracle database security management.Conclusion: through the above statements, we know the convenience and vulnerability of Oracle database. Today, data is closely related to daily life. It is very important to ensure the safety of database. Therefore, we need to maintain the security of the database from diversification and avoid the harm of Oracle database vulnerability with multiple safeguards.

5. Acknowledgment

The first author is a student from Hunan City University. This paper is directed by Professor Hean Liu.

References

[1] Telecommunications and Information Exchange between Systems–Local and Metropolitan Area Networks–Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments," IEEE Standard for Information Technology, 2018.

[2] M. Hassan, H. Vu, and T. Sakurai.Performance analysis of the IEEE 802.11 MAC protocol for DSRC safety applications. IEEE Trans. Veh.Technol., vol. 60, no. 8, pp. 3882–3896, Oct. 2018.

[3] H. Omar, W. Zhuang, and L. Li.VeMAC: A TDMA-based MAC protocol for reliable broadcast in VANETs.to be published.

[4] F. Borgonovo, L. Campelli, M. Cesana, and L. Fratta.Impact of user mobility on the broadcast service efficiency of the ADHOC MAC protocol. in Proc. IEEE VTC Spring, vol. 4, June 2017.

[5] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, and R. Herrtwich.Design of 5.9 Ghz DSRC-based vehicular safety communication. IEEE Trans.WirelessCommun., vol. 13, no. 5, pp. 36–43, Oct. 2017.