Scientific Research Publishing

Intelligent Information Management, 2022, 14, 71-79
https://www.scirp.org/journal/iim
ISSN Online: 2160-5920
ISSN Print: 2160-5912

Research and Practice on Security Protection and Disaster Recovery Strategy of Oracle Database in Colleges and Universities

Man Liu, Lei Yu*

Information Network Center, China University of Geosciences (Beijing), Beijing, China
Email: liuman@cugb.edu.cn, *yul@cugb.edu.cn

How to cite this paper: Liu, M. and Yu, L. (2022) Research and Practice on Security Protection and Disaster Recovery Strategy of Oracle Database in Colleges and Universities. *Intelligent Information Management*, **14**, 71-79.
https://doi.org/10.4236/iim.2022.142005

Received: February 14, 2022
Accepted: March 11, 2022
Published: March 14, 2022

Abstract

Database security protection, database backup and disaster recovery are important tasks for all colleges and universities to ensure the safe and stable operation of information systems. Based on the operating environment of the Oracle production database in China University of Geosciences (Beijing), combined with the practical operation and maintenance experience, this paper provides a design and implementation case of Oracle database security protection system and disaster recovery architecture. The network security protection architecture of the three-layer firewall and fortress machine, the detection and repair of security vulnerabilities, the management of system accounts and permissions, data encryption and database audit constitute the security protection system of the database. Oracle RAC (Real Application Clusters), Oracle DataGuard, redundant backup management and backup recovery constitute the disaster recovery architecture of the database. The case has practical significance for database operation and maintenance management in other colleges and universities.

Keywords

Oracle Database, Security Protection, Database Backup, Disaster Recovery, Colleges and Universities

1. Introduction

With the rapid development of information technology in colleges and universities, the teaching, scientific research and management of colleges and universities are increasingly dependent on the information platform. The database is the foundation of the information platform, so ensuring the safe and stable operation of the database is the key to the normal operation of the information platform.

The factors affecting the safe and stable operation of the Oracle database mainly come from two aspects. On the one hand, it is malicious attacks from outside, such as the intrusion to steal or destroy data, virus implantation, mining attacks, etc. On the other hand, it is the interruption of database operation or abnormal data caused by natural disasters, software and hardware failure of the database server, misoperation of managers, etc. To ensure the safe and stable operation of the Oracle database, we should focus on the above two aspects.

A lot of research and practice on the security protection and disaster recovery of the Oracle database server have been done in many universities. Most universities adopt the following methods: a two-layer firewall is used to resist attacks; regular vulnerability detection and remediation are done; Oracle RAC (Real Application Clusters) or a single machine plus Oracle DG (Data Guard) is used for disaster recovery. The above methods still have the risk of database server being attacked (such as mining), and still cannot avoid the situation that the database cannot be restored in time in extreme cases.

Based on the operating environment of the Oracle production database in China University of Geosciences (Beijing), combined with the practical operation and maintenance experience, this paper provides a design and implementation case of Oracle database security protection system and disaster recovery architecture. In this case, a three-layer firewall is used, and the fortress machine and database audit are added for security reinforcement. On the data disaster recovery level, a redundant database recovery environment is constructed based on the simultaneous use of Oracle RAC and Oracle DG.

2. Database Security Protection System

The security of the database is strengthened from different levels, such as network security protection, system vulnerability detection and remediation, database account and authority management, data encryption, database audit and so on [1] [2] [3] [4].

2.1. Network Security Protection Architecture

The network security protection architecture for database servers is shown in **Figure 1**.

Firstly, the hardware firewall A is set up between the Internet and the campus network to resist attacks and illegal access to the campus internal servers.

Secondly, all the servers in the digital campus are managed as a whole and divided into regions. The important application servers connected to the Oracle production database are integrated into a unified server region. An intranet hardware firewall B is set up in front of the server region to resist attacks and illegal access from inside the campus network. For the access of ordinary users to application servers, the firewall B only opens the corresponding service port such as 80,443. For the operation and maintenance engineers and managers, if they want to access to

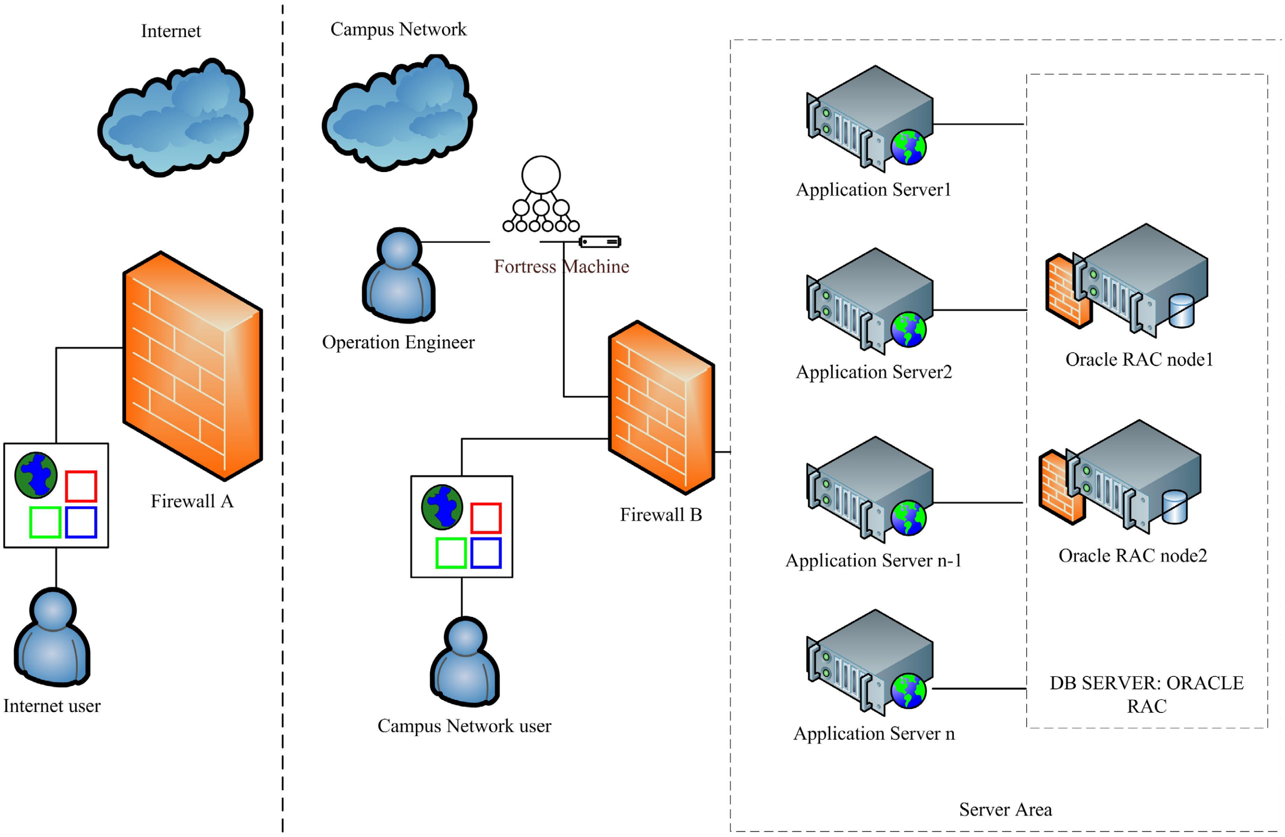

Figure 1. Database server network security protection architecture.

application servers and database servers, they have to log in to the fortress machine firstly, then the firewall B allows the fortress machine to access the management port of the target servers.

Finally, we use the software firewall on the database server and set the security policy. Only the IP address of the relevant application servers is allowed to connect to the database service port, and only the IP address of the fortress machine is allowed to connect to the database server management port.

2.2. System Vulnerability Detection and Remediation

Firstly, it is necessary to install the official patches released by Oracle in time to fix the vulnerabilities of Oracle database system itself.

Secondly, it is very important to detect the vulnerability of the operating system of the database server regularly and timely fix the medium-risk and high-risk vulnerabilities proposed in the vulnerability detection report.

For individual vulnerabilities that are difficult to fix, they can be temporarily not fixed, but they must be compensated with other security policies.

2.3. System Account and Authority Management

There are two levels of system account and authority management.

For the database server operating system, the following security policies are adopted: Prohibit the remote login of super user such as root; create ordinary users, and ordinary users log in to the system for daily transaction processing and routine maintenance; enforce complex password rules (at least 12 digits in length, including at least numbers, letters and special characters); force regular password changes.

For Oracle database system, the following security policies are adopted: for the special accounts such as sys and system, the complex password shall be changed immediately after installing the database system; modify DBA password regularly; when establishing a business user for an information system, the password must be a complex password; When authorizing a business user, the principle of minimum authority shall be followed, that is, the minimum authority shall be granted under the normal reading and writing requirements of the information system; the DBA authority shall be granted to the business user carefully; In addition, it is also necessary to withdraw expired users regularly or withdraw unnecessary permissions from users [5] [6].

2.4. Data Encryption

Data encryption is an effective means to prevent data leakage in the process of data storage and transmission. Some important and sensitive information needs encrypted storage [7]. For example, accounts and passwords of information system, ID number and so on. Of course, the encrypted stored information needs to be decrypted when the information system is displayed normally or shared with the other information system.

2.5. Database Audit

Enable the Oracle audit mechanism to monitor the user's operations on the Oracle database. By default, the audit function of the Oracle system is turned off. You can modify the value of the parameter AUDIT_TRAIL to activate the audit function. The values of AUDIT_TRAIL are shown in Table 1. After the database

Table 1. Values of the parameter AUDIT_TRAIL of Oracle database.

Value	Meaning
NONE or FALSE	Audit Disabled, Default Value
DB or TRUE	Audit Enabled, Audit Information Is Written to the Table of sys.aud$ of the Oracle Database
DB_EXTENDED	Audit Enabled, Audit Information Is Written to the Table of sys.aud$ of the Oracle Database, and Record Additional Information in the SQLBIND and SQLTEXT Fields
OS	Audit Enabled, Audit Information Is Written to the Operating System File, and the File Name is Specified by the Parameter AUDIT_FILE_DEST
XML	Audit Enabled, Audit Information Is Written to the Operating System File in XML Format

audit mechanism is enabled, an audit record is generated in the statement execution stage. The audit record contains the audit operation, the operation performed by the user, the time of the operation and other information. The database can be audited at three levels: statement, privilege and object. It is recommended that the value of the parameter AUDIT_TRAIL is set to OS or XML, and then the audit record is written to the operating system file. This configuration has less overhead on the database system.

3. Database Backup and Disaster Recovery Architecture

In addition to malicious attacks, unexpected situations such as natural disasters, hardware and software failures and manager's misoperation also occur occasionally. Therefore, only the database security protection system mentioned above is not enough, a complete database backup and disaster recovery architecture is very necessary.

Figure 2 is the backup and disaster recovery architecture of Oracle production database in the data center of China University of Geosciences (Beijing). Oracle RAC and double channel shared storage are used to eliminate the single point failure of the database, using Oracle's DataGuard technique to build an online standby database to realize rapid handover in case of RAC cluster failure. In addition to the local backup, an all-in-one backup machine is used to realize the backup management of the production database. Finally, a backup database environment for disaster recovery is built, which connects to the backup all-in-one machine and realizes the database recovery on different machine according to the actual needs.

3.1. Oracle RAC

RAC is a real-time application cluster technology for building high availability

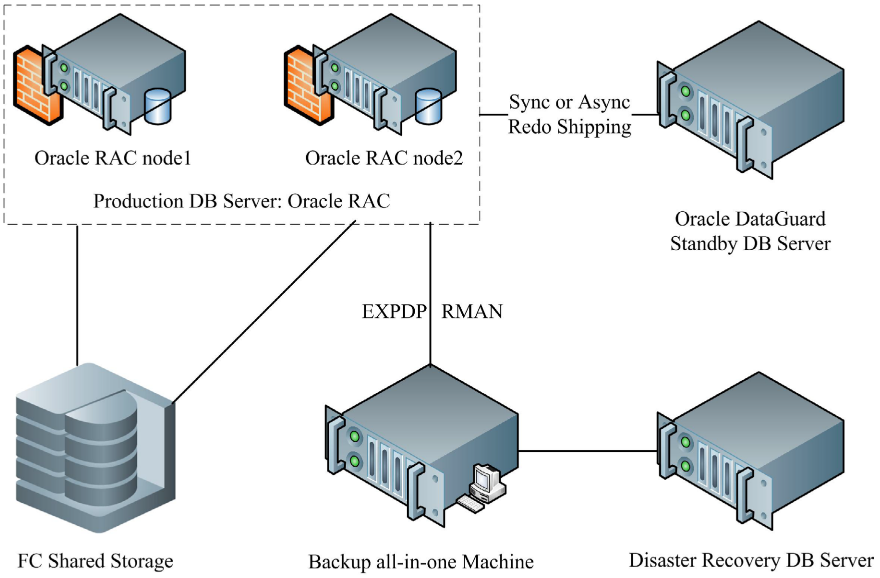

Figure 2. Database server network security protection architecture.

database systems on low-cost servers supported by Oracle in Oracle 9i and above [8]. Oracle RAC can automatically realize parallel processing and load balancing through multi-machine sharing database through cluster technology. It can also realize fault tolerance and uninterrupted recovery of database when fault occurs, so as to ensure high availability of applications. When a node in the RAC cluster fails, Oracle RAC can continue to run on its nodes without affecting the normal operation of the database. At the same time, it can also easily add nodes in the cluster to improve the system load capacity [9] [10] [11].

According to the number of information systems to be run on the database, the amount of physical data and the concurrent access of teachers and students, two Dell R840 servers are used as the database server nodes, FC double channel disk array Lenovo DE4000H is used as the shared storage, and each database server is connected to the shared storage with two HBA cards. Two database server nodes work in parallel at the same time. All database connections are assigned to two nodes for load balancing. When one server node fails, the database connections will be automatically switched to the other server node to ensure the normal operation of the information system.

3.2. Oracle DG Online Standby Database

Although Oracle RAC can eliminate single-point failure of database server, if the cluster itself or shared storage fails, it will affect the normal operation of the database, and then the business system will be interrupted, although the probability of this situation is small. In order to cope with this situation, Oracle DG technology is used to build the online backup library of RAC. Once RAC disaster occurs, it can quickly switch to the online backup library. DG protects data by data redundancy.

The working mechanism of DG is as follows: the users operate on the RAC production database, and Redo log or Archive log of the production is transmitted to the DG standby database through the network. The DG standby database redoes these logs, so as to realize the data synchronization between the production database and the DG online standby database [11] [12] [13].

Our practical experience shows that two points need to be paid attention to in the construction of DG standby database environment: first, it is suggested that the DG standby database and the RAC production library should be set in different buildings, so as to make the DG become the remote standby environment of the RAC production environment and truly solve the problem of remote disaster recovery; second, the Oracle database version installed in the DG standby database should be consistent with the RAC production database.

3.3. Data Backup Management

Even if there are RAC and DG at the same time, it is not absolutely safe. During the actual operation and management of the database, the following problems may still be encountered: first, RAC and DG fail at the same time and cannot be repaired quickly, resulting in business interruption; Second, when the information system or data of the database is abnormal, the Database Administrator (DBA) needs to query and analyze the historical data to determine the cause of the error, and then carry out targeted processing. In addition, the user's misoperation will also lead to the loss of data, at this time, it is also necessary for DBA to query the historical data to determine the time of the error, and then recover the data. To solve the above problems, we need to do a good job in the daily backup management of the database, and then complete the data recovery on the standby database according to the actual needs. Therefore, effective and recoverable data backup management is very important [11] [14] [15].

The Oracle production database of China University of Geosciences (Beijing) adopts the backup mechanism of combining local backup with remote backup and combining physical backup with logical backup and combining full backup with incremental backup. AnyBackup FX2000, a professional all-in-one backup machine, can easily complete data backup and recovery. It is recommended that the backup all-in-one machine be placed in a building different from the Oracle RAC production database. The specific backup strategies of Oracle database are shown in **Table 2**.

3.4. Standby Database for Data Recovery

A standby database environment for data recovery is built. According to the actual needs, we can use the management software of the all-in-one backup machine to recover the appropriate database physical backup files on the backup database. In case of data abnormality caused by bugs or data loss caused by user misoperation, you can select the physical backup of the corresponding date on the backup all-in-one machine and recover it on the standby database. This recovery operation solves the practical problems, but it is also a data recovery exercise, and solves the problem of physical backup data availability detection [11]

Table 2. Oracle database backup strategies.

	Physical backup(RMAN)	Logical backup(EXPDP)
Local backup (RAC)	Write backup scripts based on Oracle's RMAN, which backs up full data and archive log regularly every day; keep the full backup of the last week locally	Write backup scripts based on Oracle's Backup Data Pump, which backup full data regularly every day; keep the full backup of the last two weeks locally
Remote backup (all-in-one backup machine)	The all-in-one backup machine backs up full data and archive log regularly every day based on Oracle's RMAN; keep the full backup of the last month on all-in-one backup machine	The all-in-one backup machine backs up the logical backup files on the RAC to the all-in-one backup machine in the way of file backup; make a full backup every Sunday and an incremental backup every day from Monday to Saturday; keep the latest month's backup on the all-in-one backup machine

[16]. When the RAC production database and DG online standby database fail at the same time and cannot be repaired quickly, you can select the latest physical backup and archive log on the all-in-one machine backup for data recovery on the standby database, and then temporarily use the standby database to replace the production database to provide services.

4. Summary

The network protection architecture of three-layer firewall and fortress machine, regular vulnerability detection and repair of the database server, strict system account and authority management, intrusion detection and database audit mechanism protect the database server from attacks and minimize the risk of data leakage and data damage. The Oracle RAC technology provides a highly available, high-performance and scalable basic environment for the database. It can not only ensure the normal operation of the database system in case of failure of a single database server, but also dynamically and flexibly allocate server resources in the peak period of business, which can balance the load of high concurrency. In addition to the RAC cluster, we have established a relatively perfect disaster recovery environment. The Oracle DG online standby database is built in different places to realize immediate disaster recovery. The reliable data backup management and the standby database environment for data recovery realize data redundancy protection. The database system built by China University of Geosciences (Beijing) on the basis of the above security protection system and disaster recovery backup architecture runs stably, which effectively ensures the normal operation of various businesses of the university.

Acknowledgements

The authors thank the information network center of China University of Geosciences (Beijing) for providing a good working environment and all colleagues who provide help.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Zhang, J.X., Chen, M.L. and Wang, Q. (2010) Analysis of Web Databases-Attacking and Its Protection Strategy. *Bulletin of Science and Technology*, **26**, 769-773. https://doi.org/10.1016/S1005-0302(10)60122-3

[2] Hu, S.R., Ye, X.J., Peng, Y. and Xie, F. (2009) Design and Development of a Defense-in-Depth Model for Database Security. *Journal of Computer Research and Development*, **46**, 474-479.

[3] He, B.Y. and Liu, R. (2013) The Security Baseline Verification of Oracle and SQL Server Database. *Journal of Yunnan University* (*Natural Sciences Edition*), **35**, 63-68.

[4] He, W.C., Li, S.J., Liu, P.H., Ma, Y.J. and Yang, Y.T. (2020) Overview of Oracle Da-

tabase Security Protection. *Computer Applications and Software*, **37**, 316-322.

[5] Chen, C.J. and Yang, Y. (2003) Analysis of Web Databases-Attacking and Its Protection Strategy. *Sun Yatsen University Forum*, **23**, 208-211.

[6] Zou, X.J. (2017) Research on Database Security Technology Based on Web. Master Thesis, Beijing University of Posts and Telecommunications, Beijing.

[7] Xu, Y. (2015) Research on the Application of Sensitive Data Encryption Based on Oracle Database. *Software Engineer*, **18**, 54-56.

[8] Shi, Y.D., Gao, Q. and Hao, W.Q. (2019) Oracle Database 12c Release 2 Real Application Clusters Handbook: Concepts, Administration, Tuning & Troubleshooting. Tsinghua University Press, Beijing.

[9] Wu, B.H., Zhu, S.M. and Wu, X.Z. (2017) Application of Oracle RAC Cluster on the E-Card System of Smart Campus. *Journal of Central China Normal University* (*Natural Sciences*), **2017**, 17-20.

[10] Lv, Y.H., Sun, J.H. and Ma, L. (2016) Design and Implementation of Database Cluster System in Campus Network Based on Oracle RAC. *Modern Electronics Technique*, **39**, 72-75.

[11] Wang, Q., Liu, N.J. and Feng, K. (2011) Research on Application of Cluster and Disaster Recovery in Database of Colleges and Universities. *Experimental Technology and Management*, **28**, 91-93.

[12] Kiran, C., Abhijeet, S. and Sudhakar, J. (2015) Disaster Recovery and Zero Failover Using Oracle Dataguard. *International Journal for Scientific Research and Development*, **3**, 2048-2051.

[13] Han, W.J., Xue, J.F., Zhang, F.Q. and Sun, Z.H. (2020) An Effective Remote Data Disaster Recovery Plan for the Space TT&C System. *Machine Learning for Cyber Security*, **12487**, 31-41. https://doi.org/10.1007/978-3-030-62460-6_4

[14] Yang, F.F., Yang, X. and Ma, Q. (2017) Research on Backup Scheme of Oracle Database Based on Rman and TSM. *Computer Technology and Development*, **27**, 164-169.

[15] Antonio, R. and Lance, A. (2008) Oracle Backup and Recovery Advanced User's Guide 10g Release 2(10.2).
https://docs.oracle.com/cd/B19306_01/backup.102/b14191/title.htm

[16] Gao, G.Z., Liu, N.J., Feng, K. and Wang, Q. (2009) Research and Implementation of Oracle Standby Database Based on Backup and Restoration Technology. *Experimental Technology and Management*, **26**, 84-87.